JOYCE R. BRANDA
Acting Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

MARCIA BERMAN
Senior Trial Counsel

RODNEY PATTON
Trial Attorney

JULIA BERMAN
Trial Attorney

U.S. Department of Justice, Civil Division
20 Massachusetts Avenue, NW, Rm. 6102
Washington, D.C. 20001
Phone: (202) 514-3358; Fax: (202) 616-8470
Email: james.gilligan@usdoj.gov

Attorneys for the Government Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

CAROLYN JEWEL, *et al.*, Plaintiffs, v. NATIONAL SECURITY AGENCY, *et al.*, Defendants.	Case No. 4:08-cv-4373-JSW **GOVERNMENT DEFENDANTS' OPPOSITION TO PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT AND CROSS-MOTION FOR PARTIAL SUMMARY JUDGMENT ON PLAINTIFFS' FOURTH AMENDMENT CLAIM** Date: October 31 and December 5, 2014 Time: 9:00 a.m. Courtroom 5, Second Floor Hon. Jeffrey S. White

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES

FEDERAL RULES OF CIVIL PROCEDURE

FEDERAL RULES OF EVIDENCE

LEGISLATIVE MATERIAL

MISCELLANEOUS

INTRODUCTION

Plaintiffs filed this action six years ago alleging that the Government was then conducting "an illegal and unconstitutional program of dragnet communications surveillance" in which it acquires the phone calls and electronic communications, "both international and domestic, of practically every American . . . ." Compl. for Const. & Statutory Violations (ECF No. 1) ¶¶ 1, 9, 74-75. Plaintiffs' motion for partial summary judgment also claims at the outset to prove the existence of "an ongoing program of bulk, untargeted seizure [and search] of the Internet communications of millions of innocent Americans." Pls.' Mot. for Partial Summ. Judg. (ECF No. 261) ("Pls.' Mot.") at 1. In the end, however, Plaintiffs' motion presents a dramatically downsized case, one not supported by evidence. The "mass surveillance" depicted in their papers, *id.*, is allegedly carried out under the National Security Agency's ("NSA's") acknowledged "Upstream collection" of communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). As Plaintiffs purport to describe it, the collection involves a process by which the stream of electronic communications traveling on the fiber-optic network of a telecommunications-service provider is electronically copied, filtered to remove wholly domestic communications, and then scanned for communications containing targeted (*e.g.*, terrorist-associated) selectors, after which the copied communications *not* found to contain such selectors—*the only communications that Plaintiffs place at issue in their motion*—are destroyed within milliseconds of their creation, without ever having been seen by a human being.

Even this diminished version of the alleged "dragnet" surveillance is unsupported by admissible evidence, and fails to describe either a seizure or search, much less an unreasonable seizure or search, within the meaning of the Fourth Amendment. Plaintiffs' motion must therefore be denied, their claims dismissed, and judgment awarded instead to the Government, for numerous reasons.

First, Plaintiffs' motion should be denied as procedurally improper and unauthorized under the procedures the Court established for the orderly resolution of the four threshold questions on which the Court directed briefing. Consideration of Plaintiffs' motion for summary judgment on the merits of their Fourth Amendment claim should be deferred until the Court has

addressed both those threshold issues and the question of whether the allegations in Plaintiffs' complaint encompass the Section 702 program at all.

Second, if the Court decides to entertain the question of summary judgment at this time, then Plaintiffs' motion should be denied, their claims dismissed, and judgment awarded instead to the Government, because Plaintiffs still have not established their standing to challenge alleged ongoing collection of communications by the NSA. At the summary-judgment stage, Plaintiffs must present sufficient admissible evidence to support each essential element of their claims, including their standing, or judgment must be awarded against them. As Plaintiffs observe, the Government has acknowledged that Upstream involves the collection of certain communications as they transit the Internet backbone networks of telecommunications-service providers, but the technical details of the collection process remain classified. The Klein and Marcus declarations that form the evidentiary basis of Plaintiffs' claim that the NSA seizes and searches the online communications of millions of Americans, including theirs, rest on hearsay and speculation about activities that allegedly occurred in 2002 and 2003, and are inadmissible to prove anything about the scope, methods, or even the existence of current NSA intelligence-gathering activities, including whether Plaintiffs' communications are acquired. Moreover, although the failings of those declarations are dispositive of the standing question without implication of state secrets, the Government has also explained in briefing on the Court's four threshold questions that any attempt to adjudicate Plaintiffs' standing on grounds requiring consideration of information subject to the Government's assertion of the state-secrets privilege in this case, even in *ex parte* proceedings under 50 U.S.C. § 1806(f), risks harmful disclosure of privileged national-security information. Thus, Plaintiffs' claims must be dismissed.

Third, even if Plaintiffs had established their standing, the Government, not Plaintiffs, would still be entitled to summary judgment, because Plaintiffs have not shown as a matter of fact or law that Upstream collection involves the seizures or searches of online communications that they allege. Even if the evidence in the Klein and Marcus declarations was admissible and Plaintiffs' description of Upstream collection were accepted as true, Plaintiffs still would not succeed in demonstrating that the Government conduct assailed in their motion constitutes a

Fourth Amendment seizure or search. It is critical to understand, as Plaintiffs themselves explain, Pls.' Mot. at 8-9, that the "seizure" and "search" they complain of do not involve communications that are actually ingested by and retained in Government databases for further review and analysis by Government personnel. Rather, Plaintiffs challenge as a seizure and search, respectively, the electronic copying and scanning of those online communications that the Government does *not* retain because they are not found when scanned to contain targeted selectors. In Plaintiffs' own telling, those unretained communications are copied, scanned, and then destroyed all within a matter of milliseconds, and they are never seen by any human being. The process Plaintiffs allege does not meaningfully interfere with Plaintiffs' possessory interests in their online communications, or reveal any information about them to Government personnel. Thus, no Fourth Amendment seizure or search occurs as a matter of law.

Fourth, even if Plaintiffs had demonstrated a seizure and search of their online communications not retained by the Government, the Government must prevail under the Fourth Amendment's "special needs" doctrine. Because Upstream collection under Section 702 serves the Government's interest in collecting foreign-intelligence information for the protection of national security, information that as a practical matter cannot effectively be acquired by warrant, Upstream collection falls under the "special needs" exception to the warrant requirement. And Upstream collection meets the Fourth Amendment's essential requirement of reasonableness, because the critical importance of the intelligence-collection capabilities authorized by Section 702, as recognized by all three branches of the Government, far outweighs the vanishingly small degree (if any) to which Upstream collection under the constraints imposed by Section 702 and the Foreign Intelligence Surveillance Court ("FISC") infringes on Plaintiffs' possessory or privacy interests in online communications that the Government does not acquire.

Finally, even if the Court determined that Plaintiffs have standing, and had presented competent evidence of an unreasonable seizure or search, the state-secrets doctrine would still entitle the Government to judgment. As explained in the classified supplement and Classified Declaration of Miriam P., NSA, submitted *in camera, ex parte*, herewith, the Government possesses detailed operational information about Upstream collection that is necessary to

adjudicate Plaintiffs' Fourth Amendment claim and the Government's defenses thereto, but which is subject to the assertion of the state-secrets privilege in this case by the Director of National Intelligence ("DNI"), and cannot be disclosed without risking exceptionally grave damage to national security. In the alternative, therefore, the state-secrets doctrine requires that Plaintiffs' claims be dismissed and judgment entered for the Government.

Lacking evidence or a legal basis to support even their pared-down claim of the dragnet surveillance they once alleged, Plaintiffs repeatedly draw attention to the personal information that can be gleaned from an individual's online communications, and appeal both to the Fourth Amendment's core values and its historic purposes. But the Court need not overlook the importance of individual privacy interests or forsake the core values of the Fourth Amendment to conclude that Plaintiffs have not shown a violation of their Fourth Amendment rights. Even as Plaintiffs describe it, the Upstream process, undertaken to promote critical national-security interests, does not meaningfully encroach upon Plaintiffs' privacy or the values the Fourth Amendment is meant to protect. Plaintiffs' motion for summary judgment should be denied, their claims dismissed, and the Government's motion granted.

BACKGROUND

A. The Foreign Intelligence Surveillance Act and the FISA Amendments Act of 2008

Congress enacted FISA in 1978 to place certain types of foreign-intelligence surveillance under judicial oversight by requiring the Government to obtain an order authorizing such surveillance from a FISC judge, based on probable cause to believe, *inter alia*, that the target of the intended surveillance was a foreign power or an agent of a foreign power. *See* 50 U.S.C. §§ 1803(a), 1804(a), 1805. When Congress enacted FISA, it focused on foreign-intelligence surveillance of persons *within the United States*, *see* S. Rep. No. 95-604, at 7 (1977) (statute's purpose is "to regulate the use of electronic surveillance within the United States for foreign intelligence purposes"), by limiting the definition of "electronic surveillance," to which FISA's requirements are keyed, to domestically targeted foreign-intelligence-collection activities. 50 U.S.C. § 1801(f). Congress intentionally excluded from FISA the vast majority of Government

surveillance then conducted outside the United States, even if it targeted U.S. persons abroad, or incidentally acquired communications to or from U.S. persons or persons located in the U.S. while targeting other parties abroad. *See* S. Rep. No. 95-701, at 7, 34-35, 71 (1978).

In 2006, Congress began considering modernization of FISA because changes in communications technology had rendered its definition of electronic surveillance obsolete. *See* S. Rep. No. 110-209, at 2-5 (2007); *Modernization of the FISA: Hrg. Before the S. Select Comm. on Intel.*, 110th Cong., 1st Sess., 19 (May 1, 2007) ("May 1, 2007 FISA Mod. Hrg.") (testimony that FISA's definition of "electronic surveillance" was "tie[d] . . . to a snapshot of outdated technology"). Whereas international communications were predominantly carried by radio or satellite when FISA was enacted (and so excluded from its definition of electronic surveillance), they were now predominantly carried by fiber-optic cable, and qualified as wire communications potentially included within FISA's coverage. *Id.* at 18-19; *see* 50 U.S.C. § 1801(f)(2), (3) (defining electronic surveillance under FISA). Furthermore, intercepts of wire or other non-radio communications conducted inside the United States were covered under FISA, while those conducted outside the U.S. generally were not. May 1, 2007 FISA Mod. Hrg. at 19; 50 U.S.C. § 1801(f)(2). This was a distinction that technological advances had also rendered outmoded, when "a single communication can transit the world even if the two people communicating are only located a few miles apart." May 1, 2007 FISA Mod. Hrg. at 19. Due to these technological changes, the Government had to expend significant resources to craft numerous individual FISA applications for surveillance that was originally intended to be outside FISA's scope. *Id.* at 18.

Congress addressed this problem initially through the Protect America Act ("PAA"), Pub. L. No. 110-55 (2007), and ultimately through its successor statute, the FISA Amendments Act of 2008 ("FAA"), Pub. L. No. 110-261 (2008). The FAA provision at issue here, Section 702 of FISA, 50 U.S.C. § 1881a, "supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting . . . non-U.S. persons located abroad," *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1144 (2013), without regard to the location of the collection. Section 702 provides that, upon the FISC's approval of a "certification" submitted by the Government,

the Attorney General and the DNI may jointly authorize, for up to one year, the "targeting of [non-U.S.] persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 188la(a), (g).[1] The statute does not define this authority by reference to particular technology, other than to specify that acquisitions of communications under Section 702 must involve "the assistance of an electronic communication service provider." *Id.* § 1881a(g)(2)(A)(vi). Under the express terms of Section 702, the Government may not intentionally target any person known at the time of acquisition to be in the United States or any U.S. person reasonably believed to be located abroad, or intentionally acquire any communication known at the time of acquisition to be wholly domestic. *Id.* § 1881a(b). The acquisition must also be "conducted in a manner consistent with the [F]ourth [A]mendment." *Id.*

B. Operation of the Section 702 Program and Upstream Collection

As summarized herein, the Government has described the collection of communications under Section 702, in general terms, in a number of public reports. Upon FISC approval of a certification under Section 702, NSA analysts identify non-U.S. persons located outside the United States who are reasonably believed to possess or receive, or are likely to communicate, foreign-intelligence information designated in the certification. Such a person might be an individual who belongs to a foreign terrorist organization or facilitates its activities. NSA Civil Liberties and Privacy Office Report, NSA's Implementation of FISA Section 702 at 4 (Apr. 16, 2014) ("Civ. Lib. Report") (Exh. A hereto). Once the NSA has designated such a person as a target, it then tries to identify a specific means by which the target communicates, such as an e-mail address or a telephone number; that identifier is referred to as a "selector." Selectors may not be key words or the names of targeted individuals, but must be specific communications

[1] Four requirements must be met for FISC approval of a Section 702 certification. First, the FISC must find that the Government's "targeting procedures" are reasonably designed to ensure that acquisitions conducted under the authorization (a) are limited to targeting non-U.S. persons reasonably believed to be located outside the United States, and (b) will not intentionally acquire communications known at the time of acquisition to be purely domestic. *Id.* § 1881a(i)(2)(B). Second, the FISC must find that the Government's minimization procedures meet FISA's requirements. *Id.* §§ 1801(h), 1821(4), 1881a(i)(2)(C). Third, the Attorney General and the DNI must certify, *inter alia*, that a significant purpose of the acquisitions is to obtain foreign-intelligence information. *Id.* § 1881a(g)(2)(A)(v), (i)(2)(A). And fourth, the FISC must find that the Government's targeting and minimization procedures are consistent, not only with FISA, but also with the requirements of the Fourth Amendment. *Id.* § 1881a(i)(3)(A).

accounts, addresses or identifiers. *Id.*; Intelligence Community's Collection Programs under Title VII of the FISA at 3 ("IC's Coll. Programs") (Exh. B hereto); Privacy & Civil Liberties Oversight Bd. Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA at 32-33, 36 ("PCLOB Report") (Exhibit C hereto). An electronic-communications-service provider may then be compelled to provide the Government all information or assistance necessary to acquire communications associated with the selector, a process referred to as "tasking." PCLOB Report at 32-33; Civ. Lib. Report at 4-5.

One method through which NSA receives information concerning tasked selectors is known as "Upstream collection." Upstream collection occurs as communications "transit the Internet 'backbone' within the United States." IC's Coll. Programs at 3. *See also* PCLOB Report at 35. Under Upstream collection, tasked selectors are sent to a U.S. electronic-communications-service provider to acquire communications that are transiting the Internet backbone. PCLOB Report at 36-37. Internet communications are first filtered to eliminate potential domestic communications, and are then scanned to capture only communications containing the tasked selector. *Id*. at 37. "Unless [communications] pass both these screens, they are not ingested into government databases." *Id*. (quoted in Pls.' Mot. at 9). Further operational details regarding the mechanics of Upstream collection remain classified. *See, e.g.*, Classified Declaration of Miriam P., submitted *in camera, ex parte* herewith.

C. Plaintiff's Motion for Partial Summary Judgment

Plaintiffs' motion for partial summary judgment seeks a determination that the Government Defendants, through Upstream collection under Section 702, are currently violating the Fourth Amendment by seizing and searching Plaintiffs' Internet communications. *See* Pls.' Mot. at 1, 9, 21. Plaintiffs state that they are not, in this motion, challenging any past activities that allegedly occurred under presidential authorization, or the legality of the Government's collection of telephone communications, telephony metadata, or Internet metadata. *See id.*

The moving Plaintiffs, Jewel, Knutzen, and Walton, claim at different times to have been subscribers to AT&T's WorldNet Internet service, and they now claim to be subscribers to other AT&T Internet services. Jewel Decl. ¶¶ 2-3; Knutzen Decl. ¶¶ 2-3; Walton Decl. ¶¶ 2-3.

Although the Government has not revealed the operational details of Upstream collection and those details remain classified, Plaintiffs base their claim that Upstream collection involves unreasonable seizures and searches of their online communications on their own understanding of Upstream collection as a four-stage process.[2] First, according to Plaintiffs, their Internet-service provider, AT&T, "creates and delivers to the government" a copy of "the entire stream of domestic and international [Internet] communications" carried by AT&T's fiber optic cables, presumably including copies of their communications along with those of millions of other Americans. Pls.' Mot. at 2, 4-6, 10. Plaintiffs claim these copies are made as the communications flow through junctions (peering links) between AT&T's network and other providers' networks on the Internet backbone. *Id*. at 4 & n.3. Plaintiffs assert that the copying is accomplished using "splitters," devices that split the light signals on AT&T's fiber-optic cables to make identical copies of the communications carried on the cables. *Id*. at 6. The splitters allow a copy of the communications stream to be "diverted for further processing and searching by the NSA," while still allowing the original stream "to travel as it normally would to its intended destination on the Internet." *Id*. Plaintiffs refer to this process as "stage one" of the alleged surveillance ("Stage 1"). *Id.* at 5-6.

Next Plaintiffs assert that, at "stage two" ("Stage 2"), the copied communications are filtered for foreignness, that is, to remove purely domestic communications from the copied stream. *Id.* at 6. According to Plaintiffs, the copied and filtered communications stream is "searched" at "stage three" ("Stage 3") for particular selectors, such as email addresses and phone numbers, associated with individual targets. *Id*. at 6-9. The results are "deposited into government databases for retention" at "stage four" ("Stage 4"). *Id.* at 8. "'Only those communications . . . that contain a tasked selector'" are so retained. *Id.* at 9 n.14 (quoting PCLOB Report at 111 n.476).

Plaintiffs' evidentiary foundation for claimed Stages 1 and 2 rests on two declarations filed by Plaintiffs in 2006 in *Hepting v. AT&T*, Case No. 06-CV-0676 (N.D. Cal.): the

[2] To support their assertions regarding activities conducted at the first two stages, Plaintiffs rely on the inadmissible assertions in the Klein and Marcus declarations. As to the third and fourth stages, Plaintiffs rely largely, albeit not entirely, on facts stated about Upstream collection in Government reports, discussed *supra* at 6-7. *See* Pls.' Mot. at 6-8 & n.9, 11-14.

Declaration of Mark Klein ("Klein Decl."), a former AT&T employee who retired from AT&T in May 2004, Klein Decl. ¶¶ 2-6, and the Declaration of J. Scott Marcus ("Marcus Decl."), a purported communications technology expert, Marcus Decl. ¶ 7. Pls.' Mot. at 6 nn. 5-8. Mr. Klein claims that in 2003, AT&T constructed a new equipment room, known as the "SG3 Secure Room," at its Folsom Street telecommunications facility in San Francisco, California. According to Mr. Klein, the room was secured with multiple keyed and combination locks, and the regular AT&T technician workforce was not allowed to enter. Klein Decl. ¶¶ 11-12, 17-18. Earlier in 2002 an individual, who another AT&T employee supposedly informed Mr. Klein was an NSA agent, interviewed an AT&T Field Support Specialist for a "special job" at Folsom Street; the specialist installed equipment in the SG3 Secure Room in January 2003. *Id.* ¶¶ 10, 14. In the fall of 2003 another supposed NSA agent interviewed a second AT&T Field Support Specialist who took over the "special job" at Folsom Street in January 2004. *Id.* ¶ 16.

At this time, AT&T provided Internet services to customers through its WorldNet Internet service. *Id.* ¶ 19. Mr. Klein avers that the WorldNet Internet room at Folsom Street contained telecommunications equipment used to direct e-mails, web-browsing requests, and other Internet-based communications sent to and from customers of AT&T's WorldNet Internet service. *Id.* ¶¶ 15, 19. He asserts that in February 2003, a "splitter cabinet" was installed in the WorldNet Internet Room at Folsom Street to duplicate the signals of certain (but not all) of the fiber-optic circuits carrying WorldNet Internet services, and divert the duplicate signals to the SG3 Secure Room, while allowing the original signals to continue as they previously had. The split circuits allegedly were "peering links" that connected the WorldNet Internet network to the networks of fourteen non-AT&T telecommunications companies and two Internet exchange points. He states that the splitters transferred to the SG3 Secure Room the contents of all the electronic voice and data communications going across those links. *Id.* ¶¶ 24-34; Marcus Decl. ¶ 62. Mr. Marcus, based on his knowledge of "peering traffic patterns" in the industry, infers that the copied communications constituted all or substantially all of AT&T's off-net IP-based traffic in the San Francisco Bay Area. Marcus Decl. ¶¶ 56, 61, 71-72, 104-08.

According to Mr. Klein, an AT&T business document attached to his declaration indicates that the equipment installed in the SG3 Secure Room included a Narus STA 6400 Semantic Traffic Analyzer and a Narus Logic Server. Klein Decl. ¶ 35; *see also* Marcus Decl. ¶¶ 44, 75. Mr. Marcus opines that the Narus system was a "key component" of the SG3 equipment configuration shown on the AT&T document, "designed" to analyze large volumes of data in "real time," at "true carrier" speeds, and was "well suited" to high-speed winnowing down of large volumes of data to identify communications of interest for surveillance purposes. *Id.* ¶¶ 44, 74, 75, 79-81, 83-85. He also considers it "highly likely" that the SG3 Secure Room was connected to a second fiber-optic network other than AT&T's, on which signals could be sent out of or into the SG3 Secure Room, although he acknowledges that the documentation provided by Mr. Klein "do[es] not . . . indicate [by] what entities." *Id.* ¶¶ 76-77, 87.

Mr. Marcus also finds it "credible" that the SG3 Secure Room was intended for purposes of surveillance on a substantial scale. *Id.* ¶ 6. He opines that the infrastructure constructed at Folsom Street provided AT&T the "capacity" to assist the Government in carrying out warrantless content surveillance of both the domestic and international IP-based communications of people in the United States, with the early stages being "computer-controlled collection and analysis of communications," and the last stage being "actual human scrutiny." *Id.* ¶¶ 3, 38-39; *see also id.* ¶¶ 88, 90. The components allegedly chosen "[were] exceptionally well suited" to massive, covert surveillance of IP-based data: massive data capture with high-speed scanning at the capture point to identify data of interest, and shipment of those data to a collection point (or points) for more detailed analysis. Mr. Marcus acknowledges that the alleged configuration could have been used solely for commercial applications or routine intercepts, but in his view was vastly in excess of that needed for applications other than surveillance. The most plausible inference, he opines, is that it "was a covert network . . . used to ship data of interest to [] central locations for still more intensive analysis." *Id.* ¶¶ 40-43, 45, 47, 49, 88, 90, 129, 136.

Mr. Marcus finally opines that it is unlikely that AT&T would have made the necessary financial investments to create the SG3 infrastructure given what he characterizes as its troubled financial condition in 2003. The United States Government, he surmises, is "the most obvious

funding source," supporting the "plausibility" of a government role in the SG3 configurations. *Id.* ¶¶ 46, 137, 146, 147. He also finds it "plausible" that other splitter cabinets like the one installed at Folsom Street were installed at AT&T facilities in Seattle, San José, Los Angeles, and San Diego, and is consistent with similar deployments at 15-20 AT&T sites. He found it "highly probable" that all or substantially all of AT&T's traffic from other Internet Service Providers was diverted, including a substantial fraction, probably more than one half, of all AT&T domestic traffic, approximately ten percent of all domestic Internet communications in the United States. Klein Decl. ¶ 36; Marcus Decl. ¶¶ 113, 114, 118, 120, 124-126.

On the basis of these assertions regarding the capabilities of equipment allegedly located in a secure room at AT&T's Folsom Street facility in 2003, but without evidence of their actual use or purpose (even then), Plaintiffs contend that the Government is *today* violating their Fourth Amendment rights in two ways. First, they maintain that the Government *seizes* their online communications at Stage 1 of the Upstream process when, as they describe it, AT&T "creates and delivers to the government" a copy of "the entire stream of domestic and international [Internet-based] communications" carried on its fiber-optic network. Pls.' Mot. at 2, 6, 16-19. Second, Plaintiffs argue that after the copied communications stream is filtered, at alleged Stage 2 (the lawfulness of which they do not contest), to remove purely domestic communications, the remaining communications are *searched*, at Stage 3, to identify the communications, containing targeted selectors, that will be retained in Government databases for foreign-intelligence purposes. *Id.* at 6-9, 19-21. Plaintiffs state, without qualification, that "[t]he communications the [G]overnment retains at stage four are not at issue here," and that their motion challenges only the claimed Stage 1 "seizure of the stream of Internet communications" and Stage 3 "searching . . . of the contents of those communications for selectors." *Id.* at 9.

ARGUMENT

I. PLAINTIFFS' MOTION SHOULD BE DENIED AS PROCEDURALLY IMPROPER.

Plaintiffs' motion for summary judgment *on the merits* of their Fourth Amendment claim, as it relates to alleged ongoing seizures and searches of their Internet communications, should be

denied as procedurally improper. Plaintiffs' motion is premature in light of the threshold legal issues currently pending before the Court, and is unauthorized under the procedures the Court established for the orderly resolution of those issues.

On July 23, 2013, the Court issued a decision on the parties' prior motions to dismiss or for summary judgment, at the conclusion of which it ordered further briefing on issues pertaining, *inter alia*, to Plaintiffs' standing. *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1112-13 (N.D. Cal. 2013). The Court held a case management conference on September 27, 2013 to discuss and set a schedule for this further briefing, which the Court noted was on "important threshold legal issues." Tr. of Proceedings dated September 27, 2013 ("Tr.") at 5. The Court required additional briefing on, *inter alia*, whether Plaintiffs can establish their standing without impermissible damage to national security, assuming procedures under 50 U.S.C. § 1806(f) may be used here ("question three"). *Id*. at 6-7.

During the case management conference, counsel for Plaintiffs asked the Court whether Plaintiffs could move for partial summary judgment on "one part of one claim where we think we can prove our standing with public evidence," that is, "[their] Fourth Amendment claim" as it relates to "current ongoing internet interceptions." Plaintiffs sought leave to address this issue as part of their briefing on question three, whether they can establish their standing without risking damage to national security. *Id*. at 19-20. The Court answered that such a motion was permissible "[a]s it relates to standing." *Id*. at 20. As the transcript makes clear, the Court authorized briefing on the limited issue of whether Plaintiffs could establish their standing to bring a Fourth Amendment claim related to allegedly ongoing Internet interceptions, not full-scale summary judgment briefing on the merits of such a claim. Yet that is what Plaintiffs have filed. Plaintiffs' motion seeks to litigate the merits of one of their claims before the Court resolves the threshold legal issues it identified, in disregard of the Court's clearly stated instructions as to how the case should proceed.

In addition, the hotly disputed issue of whether Plaintiffs' complaint even includes the claim on which they purport to move for summary judgment is currently before the Court for decision. The parties have extensively briefed, in the context of their preservation dispute,

whether Plaintiffs' complaint—which alleges unlawful surveillance without any statutory or judicial authorization—even purports to challenge the legality of intelligence programs such as Upstream collection that are authorized by the FISC pursuant to Section 702 of the FISA. *See* ECF Nos. 229, 233, 235, 243, 253. As the Government has demonstrated at length, it does not. For this reason Plaintiffs are not permitted now to seek summary judgment on this unpled claim. It is "axiomatic" that claims not pled in a complaint "cannot be considered by a court at the summary judgment stage." *Feezor v. Patterson*, 896 F. Supp. 2d 895, 903 (E.D. Cal. 2012); *see also Smith v. Chase Mtg. Credit Corp.*, 653 F. Supp. 2d 1035, 1041 n.6 (E.D. Cal. 2009). At the very least, Plaintiffs' motion for summary judgment should be held in abeyance pending the Court's decision on this and the other threshold issues now pending.[3]

II. NEITHER THE KLEIN AND MARCUS DECLARATIONS NOR THE MEDIA REPORTS CITED BY PLAINTIFFS CONSTITUTE ADMISSIBLE EVIDENCE TO SUPPORT THEIR STANDING OR FOURTH AMENDMENT CLAIMS.

"One of the principal purposes of the summary judgment rule is to isolate and dispose of factually unsupported claims." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323–24 (1986). Plaintiffs must support each element of their Fourth Amendment claim, including standing, "with the manner and degree of evidence required at the successive stages of the litigation." *Bras v. Cal. Pub. Utils. Comm'n*, 59 F.3d 869, 872 (9th Cir. 1995) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992)). Plaintiffs must adduce admissible evidence establishing both their standing and the merits of their claim. *See* Fed. R. Civ. P. 56(c); *see also In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 385 (9th Cir. 2010) ("A district court's ruling on a motion for summary judgment may only be based on admissible evidence."). If Plaintiffs "fail[] to make a showing sufficient to establish the existence of an element essential to [their] case, and on which [they] will bear the burden of proof at trial," "Rule 56(c) mandates the entry of summary judgment" against them. *Celotex Corp.*, 477 U.S. at 322.

As the factual foundation for both their standing and the merits of their claims, Plaintiffs rely largely on Klein and Marcus Declarations. These declarations are the principal support for Plaintiffs' assertion that all Americans' communications—or at least all AT&T customers'

[3] If the Court nonetheless decides to entertain Plaintiffs' motion, it should, in the interests of fairness and efficiency, consider the Government's cross-motion at the same time.

communications—are currently subject to "dragnet" seizure and search. *See* Pls.' Mot. at 6. According to Plaintiffs, "[t]he Klein and Marcus evidence . . . demonstrates the NSA's bulk seizure of the content of [P]laintiffs' AT&T Internet communications from the Internet backbone." *Id.* at 10. Neither declaration provides any competent support for that claim.

A. The Klein Declaration Is Not Competent Evidence Because It Is Based on Hearsay and Speculation, Rather Than Personal Knowledge.

Rule 56(c) requires that declarations submitted in support of a summary judgment motion "be made on personal knowledge, set out facts that would be admissible in evidence, and show that the . . . declarant is competent to testify on the matters stated." Fed. R. Civ. P 56(c)(4). Thus, *inter alia*, materials must be based on the declarant's personal knowledge, *see* Fed. R. Evid. 602, rather than hearsay, *see* Fed. R. Evid. 801, 802, or speculation, *see* Fed. R. Evid. 701. *See also Stonefire Grill, Inc. v. FGF Brands, Inc.*, 987 F. Supp. 2d 1023, 1037 (C.D. Cal. 2013) (on a motion for summary judgment, "the Court may not consider inadmissible hearsay evidence which could not be presented in an admissible form at trial."); *Raglin v. UPS*, 1997 U.S. App. LEXIS 13941, at *10 ("[I]nadmissible hearsay will not be considered a 'fact' for the purposes of summary judgment.") (citing *Courtney v. Canyon Television & Appliance Rental, Inc.*, 899 F.2d 845, 851 (9th Cir. 1990)). The Klein Declaration fulfills none of these requirements.

Mark Klein, a technician employed by AT&T until 2004, executed his declaration in 2006. *See* Klein Decl. ¶¶ 2, 4. Plaintiffs rely on the Klein Declaration (and attached documents) for a description of the "SG3 Secure Room" at AT&T's Folsom Street facility, where Plaintiffs claim the Government intercepted and copied AT&T customers' Internet-based communications. *See* Pls.' Mot. at 6 nn.4–8. Mr. Klein purports to describe the installation and operation of the equipment inside that room, and to establish the Government's involvement in both. *See* Klein Decl. ¶¶ 10–35. His declaration is the sole asserted factual basis for Plaintiffs' claims in this regard; as discussed in § II.B, *infra*, Mr. Marcus, Plaintiffs' other declarant, does not purport to have independent knowledge of the Folsom Street facility and instead draws the assumptions underlying his discussion from Mr. Klein. But Mr. Klein admits he had no personal knowledge of that room's contents, or the operation of whatever equipment was installed there. According

to Mr. Klein, he did not install or operate the equipment in the SG3 Secure Room. *See id.* In fact, he "was not allowed in the SG3 Secure Room" at all. *Id.* ¶ 17. He received neither a key, nor the combination that he states was required for entry. *Id.* Mr. Klein admits he was in that room only once, for "a couple of minutes" while another technician "showed [him] some poorly installed cable." *Id.* Thus, although Plaintiffs rely on Mr. Klein to establish the content and purpose of the SG3 Secure Room, he is not qualified to offer testimony on either.

Mr. Klein claims that the SG3 Secure Room is the room into which a "splitter cabinet" diverted signals of certain fiber-optic circuits carrying AT&T customers' internet communication; he claims a copy went to the SG3 Secure Room, and the original signal continued on its path. *See id.* ¶¶ 24–34. But Mr. Klein can only speculate about what data were actually processed in the SG3 Secure Room, how, and for what purpose, since he was never involved in its operation. Indeed, having spent only a couple of minutes there, Mr. Klein cannot describe what equipment was in that room, much less explain what function it performed. Although Mr. Klein submits the document entitled "Study Group 3, LGX/Splitter Wiring, San Francisco" and claims it "list[s] the equipment installed in the SG3 Secure Room," *see id.* ¶ 35, this statement is entitled to no weight since Mr. Klein has no means of knowing that. *See id.* ¶ 17. Thus, while Mr. Klein notes that the list included "a Narus STA 6400 . . . 'Semantic Traffic Analyzer,'" *id.* ¶ 35, which Mr. Marcus claims was designed to analyze large volumes of data and was "well suited" to sort large volumes of data quickly to identify communications of interest for surveillance purposes, Mr. Klein does not claim the Narus STA 6400 was ever *actually* delivered to or installed in the SG3 Secure Room. *See* Klein Decl. ¶ 35. As with all of Mr. Klein's statements regarding the content or function of the SG3 Secure Room, any testimony about the equipment installed there should be disregarded as speculation or hearsay.

So, too, with Mr. Klein's allegations about Government involvement at the Folsom Street facility: his declaration reflects that he had no personal experience of alleged NSA activity there. Instead, his claims about Government involvement are all based on hearsay, *see* Fed. R. Evid. 801(c), 802. Although Mr. Klein asserts that "NSA cleared and approved" a particular person ("FSS #2") for a "special job," and that this person installed equipment in the SG3 Secure Room,

see id. ¶¶ 10, 14, he does not claim to have been present when that alleged clearance was issued, or to have been involved in that work. Instead, an unnamed AT&T employee allegedly told him "to expect a visit from [an] . . . NSA agent," and he received an e-mail from management that "explicitly mentioned the NSA." *Id.* ¶ 10. Such out-of-court statements, offered for the truth of the matters discussed therein, are inadmissible. So too with Mr. Klein's claim that FSS #1 told [Mr. Klein] "the NSA agent" was to interview another unnamed individual ("FSS #2") "for a special job," and FSS #1's claim that "another NSA agent would again visit" in fall 2003 to speak with FSS #3 about "tak[ing] over" FSS #2's "special job." *Id.* ¶ 16.[4]

Mr. Klein's claim regarding splitter cabinets in other AT&T locations is no different. He asserts that, while working with "another AT&T technician, [he] learned . . . 'splitter cabinets' were being installed in other cities, including Seattle, San Jose, Los Angeles and San Diego." *Id.* ¶ 36. But Mr. Klein does not purport to have ever installed, serviced, or even *seen* those alleged splitter cabinets, or to have any personal knowledge of their purpose. Such hearsay evidence is entitled to no weight on a summary judgment motion.

In sum, the Klein Declaration rests on hearsay and speculation. Such testimony is inadmissible, and is not probative even of AT&T's activities in the SG3 Secure Room, much less of any alleged nationwide Government intelligence-gathering programs.

B. The Marcus Declaration Is Not Competent Evidence Because It Offers Improper Opinion Testimony Based on the Inadmissible Klein Declaration.

Likewise, the Court should give no weight to the Marcus Declaration, which Plaintiffs offer as "an expert opinion on the implications of [the Klein Declaration its exhibits]." Marcus Decl. ¶ 1. The same provision of Rule 56(c) discussed above, applies to the Marcus Declaration; evidence relied upon on summary judgment must be admissible. *See supra* at 13. Opinion testimony from a witness proffered as an expert is admissible only if "[the] witness . . . is qualified as an expert by knowledge, skill, experience, training, or education;" "the testimony is based on sufficient facts or data;" "the testimony is the product of reliable principles and

[4] Mr. Klein asserts that NSA agents conducted the interviews discussed above, but fails to explain the basis for those statements. *See id.* ¶¶ 10, 16. Barring Mr. Klein's presence at the alleged interviews, to which he does not attest, the statements could only be based on hearsay. Likewise, his statement that "[t]o [his] knowledge, only employees cleared by the NSA were permitted to enter the SG3 Secure Room," has no apparent basis other than hearsay. *See id.* ¶ 17.

methods;" and the proffered expert "has reliably applied the principles and methods to the facts of the case." Fed. R. Evid. 702. The Marcus Declaration satisfies none of these requirements.

The Marcus Declaration was executed in 2006 by J. Scott Marcus, a consultant who had held various "positions involving computers, data communications, economics, and public policy," Marcus Decl. ¶¶ 7, 27. He also claimed he had "some experience with AT&T's network" in that, "[w]hen AT&T initially entered the Internet business in 1995," AT&T contracted with his firm to provide services to AT&T customers. *Id.* ¶ 13. Mr. Marcus did not claim to have been an AT&T employee, or to have any personal knowledge of the alleged "SG3 Secure Room." *See id.* Nonetheless, based on the Klein Declaration and its exhibits, Mr. Marcus purports to summarize "the architecture of the SG3 Configuration and its data connectivity," *id.* ¶ 64, opines on "the activities likely to be occurring" in the SG3 Secure Room, *id.* ¶ 78, and opines that the Government paid for it. *Id.* ¶ 46.

Mr. Marcus's testimony regarding the SG3 Secure Room and other AT&T facilities fails to satisfy Rule 702's requirement that a putative expert's testimony must be "based on sufficient facts or data." Fed. R. Evid. 702(b). Mr. Marcus has no personal knowledge of these facilities, and relies on the Klein Declaration regarding AT&T's operations. But, as discussed *supra*, at 14-15, that declaration is itself based on hearsay and speculation, and cannot supply the "facts" that Rule 702 requires. For this reason, Mr. Marcus's conclusions regarding the capabilities of the equipment described by Mr. Klein, or the likely uses of the SG3 Secure Room, are all speculation; there is no evidence in the record from a witness with personal knowledge of the actual contents of the SG3 Secure Room or the uses to which the equipment was put.

For example, the Court cannot rely on Mr. Marcus's discussion about the capabilities of the Narus system as a "key component" of the SG3 Secure Room, including his conclusion that it was "well suited" to high-speed winnowing down of large volumes of data to identify communications for surveillance purposes, *see* Marcus Decl. ¶¶ 44, 74, 75, 79–81, 83–85, since there is no competent evidence that such a system was actually installed or used there in the first place, *see supra* at 15. Likewise, his testimony about the "plausibility" of Mr. Klein's claims regarding splitters to be installed in other AT&T facilities only adds speculation to the hearsay

testimony of Mr. Klein, *see supra* 14-15. But on summary judgment, parties must establish the facts necessary to their claims "with the manner and degree of evidence required at the successive stages of the litigation." *Bras*, 59 F.3d at 872. The proffered evidence that Mr. Klein's inadmissible allegations are "plausible," and so could be true, falls far short of the mark.

Mr. Marcus's claim that the Government funded the SG3 Secure Room is also inadmissible, not only because it is based on Mr. Klein's inadmissible descriptions of that facility, but also because Mr. Marcus is not qualified to render such an opinion, and there is no evidence that he applied reliable methods to reach his conclusions. *See* Rule 702(c), (d). Mr. Marcus acknowledges that he "do[es] not consider [himself] an economist," Marcus Decl. ¶ 29, and he has had no economics or corporate-finance training, *see id.*, Exh. A. Mr. Marcus offers no explanation of the methods he used or the facts he relied on to assess AT&T's financial condition during the relevant timeframe, *see id.* ¶¶ 128–147, much less of their reliability, or the reliability of their application in this case. *See id.* Under Rule 702, Mr. Marcus's assessments of how AT&T would have behaved based on its financial condition, and what projects it would have funded in 2003, are not admissible evidence and therefore are not competent to support Plaintiffs' standing or Fourth Amendment claim on summary judgment.[5]

C. Even if the Klein and Marcus Declarations Were Not Based on Speculation and Hearsay, They Could Not Support Plaintiffs' Current Standing or the Merits of Their Fourth Amendment Claim.

Plaintiffs emphasize that their Fourth Amendment claim addresses *ongoing*, nationwide intelligence-gathering activities. *See* Pls.' Mot. at 1. But, even if their content were admissible, the Klein and Marcus Declarations would be probative only of events that occurred between 2002 and 2003, at least five years before Section 702 was even enacted. *See* Klein Decl. ¶¶ 10–18. Both declarations were executed in 2006, and are based on Mr. Klein's account of events that allegedly occurred ten to twelve years ago. *See id.* Because over a decade has

[5] Additionally, even if it were based on admissible evidence and the proffered expert testimony were proper under Rule 702, the Marcus Declaration is contrary to the rule that, "[i]n considering a motion for summary judgment, the court . . . is required to draw all inferences in a light most favorable to the non-moving party." *Jewel v. NSA*, 965 F. Supp. 2d 1090, 1099 (N.D. Cal. 2013) (citation omitted). Mr. Marcus repeatedly urges this Court to do just the opposite—to accept inferences uniformly favorable to the Plaintiffs' case. *See, e.g.*, Marcus Decl. ¶¶ 40, 42 (acknowledging, but asking the Court to ignore, that the SG3 Configurations could be used for commercial applications or routine intercepts).

elapsed since these alleged events, this information is too stale to be admissible. *Ortega v. O'Connor*, 146 F.3d 1149, 1162 (9th Cir. 1998) (rejecting ten-year-old complaint of improper conduct as basis for search for evidence of harassment); *see also Szajer v. City of Los Angeles*, 632 F.3d 607, 612 (9th Cir. 2010) (finding evidence five to fifteen years old "patently stale").

Similarly, while Plaintiffs ask the Court to conclude, on the strength of these declarations, that the Government's activities at "stage one" "giv[e] it access to the entire stream of domestic and international communications . . . carried on the fiber-optic cables of [the nation's leading telecommunications carriers, including AT&T]," Pls.' Mot. at 6, the information in the declarations does not extend nearly so far. Even if accepted as probative of events at the Folsom Street facility, these declarations can establish only the events at that location. For example, that Mr. Klein may have heard, from an unnamed source, of plans to install splitter cabinets in four additional AT&T locations for some unknown purpose, *see* Klein Decl. ¶ 36, cannot establish that the Internet communications of all AT&T customers, much less all Americans, are copied as part of the alleged Stage 1 process; nothing in the Klein and Marcus Declarations supports such an inferential leap.

Both as to the timeframe and the scope of the alleged intelligence-gathering activities, the Klein and Marcus Declarations fall far short of the factual showing required of Plaintiffs at the summary judgment stage of a legal proceeding.

D. The Unsubstantiated Media Reports on Which Plaintiffs Rely Constitute Inadmissible Hearsay, and Are Entitled to no Weight.

While Plaintiffs largely rely on the Klein and Marcus Declarations, they also cite a number of unsubstantiated media reports in support of their Fourth Amendment claim. *See, e.g.*, Pls.' Mot. 3–4 (discussing *Washington Post* articles); *id.* at 10 n.15 (citing articles from the *Wall Street Journal* and the *New York Times*). Such media reports are hearsay and inadmissible on a motion for summary judgment. *See, e.g., DMC Closure Aversion Comm. v. Goia*, 2014 U.S. Dist. LEXIS 121644, at *28, n.12 (N.D. Cal. Aug. 29, 2014); *Stewart v. Wachowski*, 574 F. Supp. 2d 1074, 1090 (C.D. Cal. 2005). Accordingly, the Court here should give no weight to the media reports that Plaintiffs cite.

In sum, while Plaintiffs claim the Government currently conducts "indiscriminate, suspicionless seizures" of their Internet communications, Pls.' Mot. at 25, they have come forward with no admissible evidence to support that claim. Where the party ultimately bearing the burden of proof has failed to establish the existence of an element essential to their case, Rule 56 mandates the entry of summary judgment against that party. *Celotex*, 477 U.S. at 322. The Court should enter summary judgment against the Plaintiffs here.

III. PLAINTIFFS HAVE NOT ESTABLISHED THEIR STANDING AND CANNOT DO SO WITHOUT RISK OF GRAVE DAMAGE TO NATIONAL SECURITY.

A. Plaintiffs Have Not Carried Their Evidentiary Burden of Establishing Their Standing.

As the Government has briefed numerous times in the course of this litigation, to obtain relief of any kind in this case, Plaintiffs must present "specific facts" showing that they are "among the [persons] injured" by the Government's alleged unlawful conduct. *Amnesty International*, 133 S. Ct. at 1149; *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 563 (1992) (citations and internal quotation mark omitted). That is, Plaintiffs must establish "with the manner and degree of evidence" required at the summary-judgment stage that communications of theirs are currently being seized and searched as part of NSA's Upstream collection. *Defenders of Wildlife*, 504 U.S. at 561. They have not done so.

Plaintiffs continue to assert that their communications are among those "seized" and "searched" in the course of Upstream collection based on the claim that "AT&T allows the [G]overnment to seize the entire communications stream of its customers," including Plaintiffs. Pls.' Mot. at 9-10. Plaintiffs rely entirely on the eight-year-old Klein and Marcus declarations to establish this essential fact. *Id.* at 6 nn. 5-8. But as discussed above, Mr. Klein lacks any personal knowledge of what equipment actually resided or what activities actually occurred in the "SG3 Secure Room" where he claims that copies of all or substantially all of the communications transiting the peering links at AT&T's Folsom Street facility were diverted to the NSA. Mr. Marcus attests to the capabilities of equipment that documents provided by Mr. Klein indicate were to be installed in the SG3 Room, but in the final analysis he, too, can only guess at what equipment actually was in use there, its purpose, and "what entities" had access to

communications allegedly processed there. Moreover, both individual's testimony is so outdated—concerning events that supposedly took place in 2002 and 2003—that it lacks any probative value as to ongoing activities. Because Plaintiffs have failed to adduce any admissible evidence to support this "essential element of their case," summary judgment must be awarded against Plaintiffs, not for them. *Defenders of Wildlife*, 504 U.S. at 562; *Celotex*, 477 U.S. at 322.

At best, Plaintiffs are asking the Court to speculate that Plaintiffs' communications are among those collected today based on events that allegedly occurred over a decade ago. As the Supreme Court made clear in *Amnesty International*, such speculation is an impermissible basis on which to predicate Article III standing. 133 S. Ct. at 1149.

B. Even if Plaintiffs Had Presented Admissible Evidence to Support Their Standing, the State Secrets Doctrine Would Still Require Entry of Judgment for the Government on the Standing Issue.

Due to the failings of Plaintiffs' evidence described above, the Court need not consider the impact of the state secrets privilege on the standing issue. However, if the Court were to find Plaintiffs' declarations admissible and sufficiently probative of Plaintiffs' standing to raise a genuine issue meriting further inquiry (which it should not), adjudication f the standing issue could not proceed without risking exceptionally grave damage to national security (a threshold issue on which the Court requested briefing). That is so because operational details of Upstream collection that are subject to the DNI's assertion of the state secrets privilege in this case are necessary to address Plaintiffs' theory of standing. The Government presented this evidence to the Court in the DNI's and NSA's classified declarations of December 20, 2013, and supplements it with the Classified Declaration of Miriam P., NSA, submitted *in camera, ex parte,* herewith. Disclosure of this evidence would risk informing our Nation's adversaries of the operational details of the NSA's Upstream collection, including the identities of electronic-communications-service providers assisting with Upstream collection. The risk of grave damage to national security from disclosure of this evidence remains, notwithstanding the unauthorized public disclosures and official Government releases of previously classified information about certain NSA intelligence-gathering activities since June 2013. *See* Govt. Defs.' Reply on Threshold Legal Issues (ECF No. 185) at 18-20 ("Govt.'s Reply on Threshold Issues").

Plaintiffs claim in their motion that "[n]o genuine issue of material fact exists that plaintiffs' provider AT&T is one of the Internet backbone providers at issue." Pls.' Mot. at 10. Even if that were so, it would not be sufficient to show that Plaintiffs' communications, specifically, are subject to any alleged seizure or search involved in Upstream collection. More to the point, however, the Government has already explained, in the course of the briefing on the Court's four threshold questions, that the same sources Plaintiffs point to in their instant motion as proof of AT&T's participation in Upstream collection—*e.g.*, the Klein and Marcus declarations, the decision by then-Chief Judge Walker in *Hepting v. AT&T*, 439 F. Supp. 2d 974 (N.D. Cal. 2006), and the NSA Draft Inspector General report—do not in fact prove that AT&T participates in the program or that the Government has so confirmed. Govt.'s Reply on Threshold Issues at 20-24. Indeed, as held by another member of this Court in a recent case, the identities of electronic-communications-service providers assisting with NSA intelligence-gathering activities remain classified. *Electronic Frontier Found. v. Dep't of Justice*, 2014 WL 3945646, at *5-7 (N.D. Cal. Aug. 11, 2014) (holding that identities of telecommunications-service-providers participating in the NSA's Section 215 telephony metadata program remain classified, rejecting arguments that providers' names have been officially acknowledged).

As the Court recognized in its July 23, 2013, decision, where evidence must be protected from disclosure in the interests of national security, and that information is needed to adjudicate a claim or any defenses thereto, the plaintiff's claims must be dismissed and judgment entered for the defendant. *See Kasza v. Browner*, 133 F.3d 1159, 1166 (9th Cir. 1998); *Jewel*, 965 F. Supp. 2d at 1100, 1102-03. The harm to national security here cannot be abated by holding an *in camera, ex parte* proceeding under 50 U.S.C. § 1806(f). As the Government explained in response to the Court's third question, because Plaintiffs base their standing on the claim that the entire stream of AT&T's communications, at least in the San Francisco area, is seized and searched, any adjudication of Plaintiffs' standing as a result of a § 1806(f) proceeding would necessarily reveal whether or not AT&T participates in Upstream collection, and even more specifically, whether or not AT&T's Folsom Street facility in San Francisco is involved in Upstream collection. Govt.'s Reply on Threshold Issues at 16. The Supreme Court in *Amnesty*

Int'l, 133 S. Ct. at 1149 n.4, warned against resort to an *in camera* proceeding in precisely these circumstances—where "the court's post-disclosure decision about whether to dismiss the suit for lack of standing" would reveal sensitive national security information that the proceeding was designed to protect. *See* Govt's Reply on Threshold Issues at 14-16.

For these fundamental reasons, Plaintiffs have not established their standing to raise a Fourth Amendment claim based on Upstream collection. Alternatively, even if they had presented sufficient evidence of their standing to raise a genuine issue regarding their standing, the question cannot be litigated without potentially harmful disclosures of privileged national-security information. Plaintiffs' motion for summary judgment must therefore be denied, their claims dismissed, and judgment awarded to the Government.

IV. PLAINTIFFS SHOULD BE DENIED SUMMARY JUDGMENT, AND JUDGMENT SHOULD INSTEAD BE AWARDED TO THE GOVERNMENT, ON THE MERITS OF PLAINTIFFS' FOURTH AMENDMENT CLAIM.

A. Plaintiffs' Claim of a Seizure at "Stage 1" Fails as a Matter of Fact and Law.

The first of the two Fourth Amendment violations asserted by Plaintiffs is that the Government unconstitutionally, through Upstream collection authorized under Section 702 (and FISC orders) seizes their Internet-based communications (and those of millions of other Americans) by obtaining copies automatically created and then delivered to the Government by their Internet service provider, AT&T. Pls.' Mot. at 2, 16-19. The alleged seizure occurs at what Plaintiffs designate "stage one" of "the [G]overnment's surveillance process," where they maintain the Government "taps into the Internet backbone networks of the nation's leading telecommunications carriers, including AT&T," to obtain "access to the entire stream" of Internet-based domestic and international communications. According to Plaintiffs, this alleged interception and copying of the "communications stream" is "a general seizure that is not, and never could be, authorized by a valid warrant." *Id.* at 6, 16.

Plaintiffs' application for summary judgment on this claim must be denied, and judgment awarded instead to the Government, for two reasons: (1) Plaintiffs have adduced no admissible evidence to support the contention that the NSA's "Upstream" collection of communications involves the interception and copying of the entire communications stream carried by AT&T (or

any other provider); and (2) even if Plaintiffs' evidence—the "facts" asserted in the Klein and Marcus declarations—were taken at face value, the conduct ascribed to the Government does not, as a matter of law, constitute a Fourth Amendment seizure.

1. Plaintiffs have presented no admissible evidence that Upstream collection under Section 702 in fact involves the "Stage 1" seizure they allege.

As discussed above, the Government has acknowledged that pursuant to Section 702 it engages in targeted "Upstream" acquisition of communications as they "transit the Internet 'backbone'" networks of telecommunications-service providers within the United States." IC Coll. Pgms. at 3; *see supra* at 6-7. The Government has not disclosed, however, the technical details of the means by which providers make these targeted communications available to the Government. Those operational details remain classified.

As support, therefore, for their allegations that the Government intercepts and copies the entire communications stream from AT&T's Internet backbone network—the very essence of their seizure claim—Plaintiffs rely exclusively on the attestations of the Klein and Marcus declarations. *See* Pls.' Mot. at 6 & nn. 4-8. As discussed *supra*, § II, nothing that Messrs. Klein and Marcus say about the Government's alleged interception and copying of Internet-based communications at AT&T's Folsom Street facility constitutes admissible evidence. Moreover, the information on which both declarants rely about the SG3 Secure Room in 2003 is now more than a decade old, and relates to alleged events occurring years before Section 702 was enacted. It is therefore not probative of any intelligence activity in which the Government *currently* engages, *see supra* at 18-19—the exclusive concern, as Plaintiffs themselves state, of their request for summary judgment. Pls.' Mot. at 1. Thus, Plaintiffs have failed to adduce any competent evidence that Upstream collection, or any other Government intelligence program, involves the interception and copying of the entire communications stream from AT&T's (or any other provider's) Internet backbone network, and so doing have presented no evidence to support an essential element of their seizure claim as they have defined it. For this simple reason if no other the Government, not Plaintiffs, is entitled to judgment on Plaintiffs' seizure claim. *Celotex*, 477 U.S. at 322.

2. Even if proven, the alleged "Stage 1" splitting of the Internet communications stream would not constitute a Fourth Amendment seizure as a matter of law.

Even if the Klein and Marcus declarations could be accepted as evidence of ongoing Government conduct, the Government would still be entitled to judgment on Plaintiffs' seizure claim as a matter of law. Plaintiffs allege surveillance involving the real-time interception and copying of electronic communications, without delay or interruption in their flow, followed by filtering for foreignness and scanning for targeted selectors, whereupon, as discussed below, the communications at issue here are destroyed within milliseconds of their creation without retention by the Government. This process does not involve a seizure for which a warrant or probable cause is required, because it does not constitute a Fourth Amendment "seizure" at all.

An evaluation of Plaintiffs' seizure claim must begin with an understanding of what constitutes a seizure for purposes of the Fourth Amendment, a subject bypassed in Plaintiffs' motion. The Fourth Amendment assures the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend IV, cl. 1. As the Supreme Court and the Ninth Circuit have explained, "[d]ifferent interests are implicated by a seizure than by a search. A seizure affects only [a] person's possessory interests; a search affects a person's privacy interests." *Segura v. United States*, 468 U.S. 796, 806 (1984) (citations omitted); *United States v. Jacobsen*, 466 U.S. 109, 113 (1984); *Texas v. Brown*, 460 U.S. 730, 747-48 (1983) (Stevens, J., concurring); *United States v. Jefferson*, 566 F.3d 928, 933 (9th Cir. 2009). Accordingly, a Fourth Amendment seizure of property occurs "when there is some meaningful interference with an individual's possessory interests in that property." *Jacobsen*, 466 U.S. at 113; *Jefferson*, 566 F.3d at 933. "'Absent such interference, no fourth amendment seizure will be found.'" *DeBoer v. Pennington*, 206 F.3d 857, 865 (9th Cir. 2000) (quoting *United States v. England*, 971 F.2d 419, 420 (9th Cir. 1992)). *See also, e.g., United States v. Clutter*, 674 F.3d 980, 984-85 (8th Cir. 2012); *United States v. Va Lerie*, 424 F.3d 694, 708 (8th Cir. 2005) (no seizure where temporary removal of bus passenger's checked luggage during a re-fueling stop did not meaningfully interfere with his possessory interests); *United States v. Elmore*, 304 F.3d 557, 560-61 (6th Cir. 2002); *United States v. Brown*, 884 F.2d 1309,

1311 (9th Cir. 1989) ("[n]o seizure occurred" when detectives arranged to have airline passenger's checked suitcases held while they obtained his permission to search them).

Plaintiffs do not explain what *possessory* interest they have in the "communications stream"—modulated electromagnetic impulses moving at the speed of light across fiber-optic networks—but it is clear no meaningful interference with any such interest occurs at Stage 1 of the surveillance process they allege, which involves no interruption or delay of communications they send or receive, or retention by the Government of the copied communications that Plaintiffs identify as the subject of their motion.

Plaintiffs maintain that due to similarities between electronic communications such as e-mail and traditional forms of communication such as letters and telephone calls, electronic communications are entitled to similar Fourth Amendment protection. Pls.' Mot. at 11-14. But Plaintiffs do not benefit from that analogy. The Ninth Circuit, together with other courts of appeals, has repeatedly held that the possessory interest protected by the Fourth Amendment in mailed (or privately shipped) letters and packages is "solely in [their] timely delivery." *United States v. Jefferson*, 566 F.3d 928, 933-34 (9th Cir. 2009); *United States v. Hoang*, 486 F.3d 1156, 1160 (9th Cir. 2007). Accordingly, the Court of Appeals has held that no Fourth Amendment seizure occurs unless the government's temporary detention of a mailed letter or package, once in transit, "significantly interfere[s] with [its] timely delivery in the normal course of business." *Hoang*, 486 F.3d at 1162 & nn. 2-3 (ten-minute detention of FedEx package for purpose of canine narcotics sniff that did not interfere with package's scheduled delivery did not implicate the recipient's Fourth Amendment rights) (citing, *inter alia*, *United States v. Zacher*, 465 F.3d 336, 338-39 (8th Cir. 2006) and *United States v. LaFrance*, 879 F.2d 1, 7 (1st Cir. 1989)); *see also Jefferson*, 566 F.3d at 934-35 (citing *United States v. Gill*, 280 F.3d 923, 932-33 (9th Cir. 2002) (Gould, J., concurring)) ; *United States v. England*, 971 F.2d 419, 420-21 (9th Cir. 1992) (citing *United States v. Place*, 462 U.S. 696, 718 n.5 (1983) (Brennan, J., concurring) ("mere detention of mail not in [the defendant's] custody or control amounts to at most a minimal or technical interference with his person or effects, resulting in no deprivation at all")).

The "Stage 1" duplication of electronic communications alleged by Plaintiffs results in no demonstrated delay in the delivery of anyone's communications; indeed, Plaintiffs themselves explain that the purpose of the electronic copying that they condemn as a "seizure" is to *avoid* "interrupting or slowing Internet communications" by "allow[ing] one copy of the [duplicated] communications stream to travel as it normally would to its intended destination on the Internet." Pls.' Mot. at 6; *see also* Marcus Decl. ¶¶ 62, 72-73. Thus, by Plaintiffs' own telling, Stage 1 causes no delay in the communications that Plaintiffs send or receive, as would be required to demonstrate a seizure under the traditional Fourth Amendment principles Plaintiffs invoke.

Moreover, because the communications at issue are not retained by the Government, Plaintiffs' claim is also undermined by precedent holding that no seizure takes place when law-enforcement officers momentarily pick up an item or move it a short distance for the purpose of a brief visual or other non-intrusive form of inspection. For example, in *United States v. Hall*, 978 F.2d 616 (10th Cir. 1992), a narcotics agent proceeded to the luggage area of the train on which a suspected drug courier was traveling and lifted her suitcase from the bin in which it had been stowed. Finding the bag suspiciously heavy, the agent detained it for an intended canine sniff test and, ultimately, a search revealing 40 pounds of marijuana inside. *Id.* at 618-19. The court held that the agent's initial "lifting of [the] suitcase did not constitute a seizure because this interference with [the courier's] possessory interests in her suitcase was minimal." *Id.* at 619. In reaching this conclusion, the court relied on *Arizona v. Hicks*, 480 U.S. 321 (1987), *see Hall*, 978 F.2d at 619-20, where the Supreme Court held that turning over a piece of stereo equipment to read and record its serial number did not "[i]n and of itself" amount to a seizure because "it did not meaningfully interfere with [the defendant's] possessory interest in either the serial number or the equipment." *Hicks*, 480 U.S. at 324 (citation and quotation marks omitted). *See also United States v. Schofield*, 80 Fed. Appx. 798, 802-03 (3d Cir. 2003) (officer "almost certainly did not seize" box by lifting it during search of car trunk); *United States v. DeMoss*, 279 F.3d 632, 634-36 (8th Cir. 2002) (officer did not seize passing package when he lifted it from conveyor belt); *United States v. Gant*, 112 F.3d 241-42 (6th Cir. 1997); *United States v. Harvey*, 961 F.2d 1361, 1363-64 (8th Cir. 1992).

The Stage 1 copying of communications that Plaintiffs allege, for the subsequent purpose of real-time filtering for foreignness and scanning to detect communications containing lawfully targeted selectors, is analogous to "pick[ing] up an individual's property to look at it," and likewise results in no seizure because "th[e] interference with the [communicant's] possessory interest" in the communication "is not meaningful." *Hall*, 978 F.2d at 619. Plaintiffs and their expert, Mr. Marcus, posit a surveillance process by which millions of Americans' Internet-based communications are copied, filtered for foreignness, and scanned for targeted selectors in "real time," at "true carrier speeds," as those communications propel across providers' fiber-optic networks at incomprehensible speed. Pls.' Mot. at 6-8; Marcus Decl. ¶¶ 80, 83. Ultimately some of those communications (those found at Stage 3 to contain targeted selectors) are stored in Government databases (at Stage 4), but that is not the "seizure" complained of; Plaintiffs expressly state that "[t]he communications the [G]overnment retains at stage four are not at issue here." Pls.' Mot. at 8-9. Rather, Plaintiffs contest the legality of the alleged seizure of those communications that are not retained in Government databases (because they are not found to contain targeted selectors). But because, under the scenario described by Plaintiffs, these communications are copied, filtered for foreignness, and scanned for targeted selectors in real time as the communications stream at the speed of light, the copies could exist for no more than milliseconds before being discarded or destroyed. There is no meaningful interference with any possessory interest articulated by Plaintiffs that results from the Government's alleged possession of these copied communications for literally thousandths of a second.

The almost instantaneous destruction of the copied communications once they are made distinguishes the scenario alleged by Plaintiffs from situations where government authorities obtain copies of individuals' electronic information—such as e-mails stored on a provider's server, or data contained on a laptop computer—and retain it in government databases for investigatory purposes. In such cases, some courts have held that the government's acquisition and indefinite retention of the copied data constitutes a seizure, because "an individual's possessory interest in [such data] extends to both the original and any copies made from it." *See, e.g.*, *In re Search of Info. Associated with [Redacted] at mac.com [etc.]*, 2014 WL 1377793, at

*2, 3 (D.D.C. Apr. 7, 2014), *vacated on other grounds*, 2014 WL 4094565 (D.D.C. Aug. 8, 2014); *United States v. Saboonchi*, 990 F. Supp. 2d 536, 565 (D. Md. 2014). In other such cases, courts have held that no seizure occurs because although the government has obtained a copy, the original dataset remains accessible to the owner and as a result no meaningful interest with his or her possessory interest results. *See, e.g.*, *In re Application of the United States of America for a Search Warrant for Contents of Electronic Mail [etc.]*, 665 F. Supp. 2d 1210, 1222 (D. Or. 2009); *United States v. Gorshkov*, 2001 WL 1024026, at *3 (W.D. Wash. May 23, 2001) (citing *Hicks*, 480 U.S. at 324). But regardless of which view the law ultimately embraces, the situation alleged by Plaintiffs here is materially different from these cases, because they have specified that their claim concerns copies of communications data that the Government does not retain, and which, once created, are almost immediately destroyed. Plaintiffs identify no meaningful interference with their possessory interest in these copied communications that could possibly occur during the vanishingly brief moment of their existence. The copying of communications data that allegedly occurs at Stage 1 is therefore not a seizure.

3. No authority cited by Plaintiffs supports their seizure claim.

For their part, Plaintiffs cite no authority to support the proposition that Upstream collection involves a seizure of their online communications. First they attempt to equate the alleged electronic copying of a communications data stream with general warrants and writs of assistance, the historic instruments of British oppression that the Fourth Amendment was most urgently intended to prohibit. *See Virginia v. Moore*, 553 U.S. 164, 168-69 (2008); Pls.' Mot. at 17-18. As the Supreme Court has summarized their history, general warrants were employed by the British Crown to authorize the arrest of all persons suspected of authoring, printing, or distributing seditious publications, together with the seizure of all their personal papers; writs of assistance were issued in pre-revolutionary times to give British officers blanket authority to barge into colonists' homes in unrestrained search for illegally imported goods. *See Stanford v. Texas*, 379 U.S. 476, 481-82 (1965); *Marcus v. Search Warrants of Property*, 367 U.S. 717, 726-29 (1961); *see also Riley v. California*, 134 S. Ct. 2473, 2494 (2014). No amount of argument on Plaintiffs' part can succeed in equating the installation of fiber-optic splitters on

telecommunications cables far removed from Plaintiffs' homes, to create copies of electronic data that are then almost instantaneously destroyed, as the legal equivalent of these historic offenses against personal liberty.[6]

There are likewise no valid parallels to be drawn between the transitory creation and destruction of copied communications at Stage 1 with the entry upon the defendants' places of business and the physical seizures (and retention) of all their business records in *United States v. Tamura*, 694 F.2d 591, 594-95, 596-97 (9th Cir. 1982) and *United States v. Kow*, 58 F.3d 423, 425 (9th Cir. 1995). *See* Pls.' Mot. at 17. Alleged Stage 1 copying of the communications stream does not involve the wholesale physical confiscation from Plaintiffs' possession of their personal papers or business records, but at best a fleeting grasp and release of electronic data transiting distant fiber-optic cables, without impeding the journeys of Plaintiffs' communications to their intended destinations on the global communications network. As the process described by Plaintiffs results in no meaningful interference with any possessory interest Plaintiffs have in their electronic communications, it is not a Fourth Amendment seizure and requires neither a warrant, nor individualized suspicion.[7]

[6] The fact that the data actually retained by the Government are "not at issue here," Pls.' Mot. at 9, also eliminates any valid basis for comparing Stage 1 of the alleged surveillance process here to the NSA's Cold War-era "Operation Shamrock," or for Plaintiffs' continued reliance on this Court's prior decision in *Hepting v. AT&T*, 439 F. Supp. 2d 974 (N.D. Cal. 2006), *id.* at 16-17, 18. *See* Intelligence Activities: Hrgs. Before the Sen. Select Comm. To Study Governmental Operations With Respect to Intelligence Activities, 94th Cong., Vol. V, 57-59 (1975) (statement that during Operation Shamrock NSA acquired and NSA analysts sorted through most international telegrams originating in or forwarding through the United States), *available at* http://www.intelligence.senate.gov/pdfs94th/94intelligence_activities_V.pdf; *Hepting*, No. 3:06-cv-00672-VRW, First Amended Compl. ¶¶ 42-46 (ECF No. 8) (alleging that all or substantially all of the communications transmitted through AT&T's key domestic telecommunications facilities were actually acquired by the Government).

[7] Plaintiffs confuse the issue when they assert, in support of their seizure claim, that they have a reasonable expectation of privacy in the copied communications. Pls.' Mot. at 17. By definition, the violation of an individual's reasonable expectation of privacy constitutes a search, not a seizure, *see Segura*, 468 U.S. at 806; *Jacobsen*, 466 U.S. at 113, but Plaintiffs do not contend that electronic copying of their communications in and of itself constitutes a search. Rather, Plaintiffs contend that the alleged duplication of the communications stream is a seizure, which requires a meaningful interference with a possessory interest. Plaintiffs' reliance on *Florida v. Jardines*, 133 S. Ct. 1409 (2013), and *United States v. Jones*, 132 S. Ct. 945 (2012), *see* Pls.' Mot. at 17, suffers from the same confusion, as both are "search," not "seizure" cases.

B. Plaintiffs' Claim That Alleged "Stage 3" Scanning Constitutes a Search of Communications Not Found To Contain Targeted Selectors Is Also Without Merit.

Plaintiffs' second contention is that scanning copied communications at "Stage 3" (after they are filtered for foreignness) for those that contain targeted selectors constitutes a Fourth Amendment search. Pls.' Mot. at 19-21. In contrast to a seizure, which involves governmental interference with a possessory interest, a Fourth Amendment search occurs when the government obtains information by physically intruding on a constitutionally protected area, or by violating a person's reasonable expectation of privacy. *Jardines*, 133 S. Ct. at 1414; *Jones*, 132 S. Ct. at 949-50. Plaintiffs devote a great deal of effort to establishing that they have a reasonable expectation of privacy in their Internet-based communications. Pls.' Mot. at 11-14. One need not quarrel with the proposition to conclude, nonetheless, that no search of Plaintiffs' online communications has been demonstrated. Where the official conduct complained of "does not 'compromise any legitimate interest in privacy' [it] is not a search subject to the Fourth Amendment." *Illinois v. Caballes*, 543 U.S. 405, 408 (2005) (quoting *Jacobsen*, 466 U.S. at 123). That is the case here so far as the communications at issue are concerned.

As discussed *supra*, at 28, Plaintiffs and their expert describe Upstream collection as a process by which millions of communications are copied, filtered for foreignness and scanned for targeted selectors in real time, through the use of sophisticated electronic equipment capable of processing large volumes of communications data to identify "traffic of interest." Pls.' Mot. at 6-8; Marcus Decl. ¶¶ 79-85. Only afterward, at "Stage 4," are the results of this filtering and scanning allegedly "deposited into [G]overnment databases for retention" and "actual human scrutiny." Pls.' Mot. at 8; Marcus Decl. ¶ 39. But the copied communications retained at Stage 4 are "not at issue," *id.* at 9; the only copied communications at issue are those discarded, within milliseconds of their creation, because they are not found as a result of the electronic scanning to contain targeted selectors. Plaintiffs do not allege, much less do they submit admissible evidence to prove, that any information about these discarded communications, including communications of theirs, is provided to Government officials before they are destroyed. They do not explain, for that matter, how Government personnel could know even of

the existence of any communications in which Plaintiffs or any other U.S. persons engage if they are not among the targeted communications retained at Stage 4.

In this respect—that is, the utter lack of information made available to Government personnel—the alleged scanning of unretained communications resembles the narcotics-dog sniff of luggage, and the chemical field test for cocaine, that the Supreme Court held did not constitute Fourth Amendment searches in *United States v. Place*, 462 U.S. 696, 706-07 (1983) and *Jacobsen*, 466 U.S. at 123-24, respectively. In *Place*, DEA agents, suspecting an airline passenger of transporting illegal narcotics, took his luggage from his possession and transported his bags to another location for a "sniff test" by a trained narcotics-detection dog. The dog alerted to one of the bags, after which the agents, upon obtaining a search warrant, opened the bag and discovered more than a kilogram of cocaine inside. 462 U.S. at 698-99. Although ultimately concluding that Place's luggage had been unconstitutionally seized, the Supreme Court first concluded that subjecting the luggage to the canine sniff test did not constitute a search within the meaning of the Fourth Amendment. The Court explained:

> A "canine sniff" by a well-trained narcotics detection dog . . . does not require opening the luggage. *It does not expose noncontraband items that otherwise would remain hidden from public view*, as does, for example, an officer's rummaging through the contents of the luggage. Thus, the manner in which information is obtained through this investigative technique is much less intrusive than a typical search. Moreover, the sniff discloses only the presence or absence of narcotics, a contraband item. Thus, despite the fact that the sniff tells the authorities something about the contents of the luggage, the information obtained is limited. This limited disclosure also ensures that the owner of the property is not subjected to the embarrassment and inconvenience entailed in less discriminate and more intrusive investigative methods.

Id. at 707 (emphasis added).

The Court extended the logic of *Place* to a chemical test for narcotics in *Jacobsen*. In that case, employees of a private freight carrier, upon discovering a white powdery substance inside a damaged package, summoned federal narcotics agents. Upon arriving, the agents made an "on the spot" chemical field test that identified the substance as cocaine, leading to the arrest and conviction of the package's intended recipients. *Jacobsen*, 466 U.S. at 111-12 & n.1. The Court held that the chemical test did not constitute a Fourth Amendment search, because it "could disclose only one fact . . . whether or not a suspicious white powder was cocaine"—

"nothing more"—and therefore "d[id] not compromise any legitimate interest in privacy." *Id.* at 122-23. "[E]ven if the results are negative," the Court emphasized, "such a result reveals nothing of special interest." *Id.* at 123. The Court observed further that its conclusion was "dictated" by the decision in *Place,* because the chemical test, like a narcotics-dog sniff, "could reveal nothing about noncontraband items." *Id.* at 123-24 & n.24.

The logic underlying the decisions in *Jacobsen* and *Place* applies equally to Stage 3 scanning of communications that do not contain targeted selectors. So far as Plaintiffs maintain or prove, electronic scanning at Stage 3 of communications that are not found to contain targeted selectors results in their immediate destruction, without revealing anything about them to the Government. Indeed, the information gleaned about unretained communications is even less than the modicum of information revealed either by the canine sniff in *Place* or the chemical field test in *Jacobsen.* As the Court observed in *Place*, if the narcotics-detection dog does not alert, that "tells the authorities something about the contents of the luggage" (the absence of illegal drugs) but that information is too "limited" to raise the intrusion to the level of a search. 462 U.S. at 707. Likewise, a negative chemical field test reveals "that [a] substance is something other than cocaine," but that disclosure, too, is of insufficient "interest" to result in a search. *Jacobsen*, 466 U.S. at 123. Here, so far as Plaintiffs' evidence indicates, if Stage 3 scanning of a copied communication is negative the Government learns nothing about it—not even that it exists. Accordingly, so far as Plaintiffs' motion concerns only communications that have not been found to contain targeted selectors, they have not shown that Government personnel obtain any information about Plaintiffs' communications, the contents thereof, or with whom Plaintiffs communicate online. Thus, under the rationales of *Place* and *Jacobsen*, Plaintiffs have made no showing that Stage 3 scanning of their communications "'compromise[s] any legitimate interest [of theirs] in privacy,'" *Caballes*, 543 U.S. at 408 (quoting *Jacobsen*, 466 U.S. at 123), and so have not demonstrated the occurrence of a Fourth Amendment search.

Plaintiffs seek to support the opposite conclusion by again invoking historic memory of general warrants and writs of assistance, likening the electronic scanning of communications data copied from fiber-optic cables to a "'general exploratory rummaging'" of every colonist's

home by British troops. Pls.' Mot. at 20-21. The comparison is ill-conceived, however, and its logical flaw is exposed by the Court's reasoning in *Place*. There the Court explained that a narcotics-dog sniff is distinguishable from "an officer's rummaging through the contents of [an individual's] luggage," because a sniff test does not expose items, other than targeted narcotics, "that otherwise would remain hidden from public view." 462 U.S. at 707. Thus "the owner of the property is not subjected to the embarrassment and inconvenience entailed in less discriminate and more intrusive investigative methods." *Id*. As in *Place*, communications not found at Stage 3 to contain targeted selectors "remain hidden," so far as Plaintiffs have demonstrated, from the Government's view, *id.*, and no search of those communications, much less the equivalent of a house-to-house search of the entire thirteen colonies, takes place. The Government, not Plaintiffs, is entitled to judgment on Plaintiffs' search claim as a matter of law.

C. The "Stage 1" Seizure and "Stage 3" Search Alleged by Plaintiffs Fall Within the Fourth Amendment's "Special Needs" Doctrine and Are Reasonable Under the Totality of the Circumstances.

Even if the alleged real-time copying and scanning of Plaintiffs' electronic communications at Stages 1 and 3 constituted seizures and searches within the meaning of the Fourth Amendment, these activities serve special Government needs and, therefore, under settled doctrine, do not require a warrant. They are reasonable under the totality of the circumstances—reflecting Congress's and the Executive's careful balancing of the relevant national-security and privacy interests—and are therefore constitutional, because their importance to national security far outweighs any minimal intrusion they impose on Plaintiffs' Fourth Amendment interests.

1. The challenged surveillance activities do not require the issuance of a warrant upon probable cause because the Government has a "special need" to collect foreign-intelligence information.

Plaintiffs argue that the alleged Stage 1 copying and Stage 3 scanning of their communications violate the Fourth Amendment because "[n]ational security does not excuse the need for a warrant" to conduct these activities. Pls.' Mot. at 14. But under the Supreme Court's "special needs" doctrine, it does. The "touchstone" of Fourth Amendment analysis "is always 'the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security.'" *Pennsylvania v. Mimms*, 434 U.S. 106, 108-09 (1977) (per curiam)

(quoting *Terry v. Ohio*, 392 U.S. 1, 19 (1968)). "[A]lthough 'both the concept of probable cause and the requirement of a warrant bear on the reasonableness of a search,'" *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985) (citation omitted), "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance," *National Treas. Emp. Union v. Von Raab*, 489 U.S. 656, 665 (1989). In fact, "the traditional probable-cause standard may be unhelpful" when the Government "seeks to *prevent*" dangers to public safety. *Id.* at 668.

The Supreme Court has recognized exceptions to the warrant requirement in a variety of circumstances, including where "special needs, beyond the need for law enforcement, make the warrant and probable-cause requirement impracticable," *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987), and the needs are motivated "at [a] programmatic level" by other governmental objectives. *See City of Indianapolis v. Edmond*, 531 U.S. 32, 37-40, 48 (2000). Under the "special needs" doctrine, the Fourth Amendment instead requires courts to "employ[] a balancing test that weigh[s] the intrusion on the individual's [constitutionally protected] interest[s]" against the "'special needs' that support[] the program." *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001).[8]

A number of courts have held that the Government's "special need" for foreign-intelligence information justifies an exception to the warrant requirement. *See, e.g.*, *United States v. Duka*, 671 F.3d 329, 340-45 (3d Cir. 2011); *In re Directives*, 551 F.3d 1004, 1010-12, (FISC Ct. Rev. 2008); *United States v. Truong Dinh Hung*, 629 F.2d 908, 912-16 (4th Cir. 1980); *United States v. Mohamud*, 2014 WL 2866749, at *15-18 (D. Or. June 24, 2014); *Cf. United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977) ("Foreign security wiretaps are a recognized exception to the general warrant requirement . . . .").

The rationale for these decisions derives from *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297, 322 (1972), a case involving electronic surveillance for domestic security

[8] Under the "special needs" doctrine, the Supreme Court has permitted warrantless stops at roadblocks to secure borders, *United States v. Martinez-Fuerte*, 428 U.S. 543, 566-67 (1976), warrantless searches of probationers' homes to ensure compliance with probation conditions, *Griffin*, 483 U.S. at 872-75, and warrantless searches of public school students to enforce school rules, *T.L.O.*, 469 U.S. at 340.

purposes, *id.* at 299. Although the Supreme Court there held that "prior judicial approval" was required for "the type of domestic security surveillance" at issue in that case, *id.* at 324, the Court recognized that, due to the significant differences between national-security investigations and ordinary criminal investigations, different standards for intelligence surveillance "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights" of citizens. *See id.* at 322-23; *Duka*, 671 F.3d at 339-41. The courts that have since addressed the issue of whether the collection of foreign-intelligence information requires a warrant—an issue the Supreme Court specifically reserved, *Keith*, 407 U.S. at 308, 322-23—have expressly distinguished *Keith's* facts in holding that it does not. *See In re Directives*, 551 F.3d at 1010; *In re Sealed Case*, 310 F.3d 717, 744 (FISA Ct. Rev. 2002); *Truong*, 629 F.2d at 913. *Cf. Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013) (noting that *Keith* "implicitly suggested that a special framework for foreign intelligence surveillance might be constitutionally permissible").[9]

In concluding that no warrant is required in this context, the courts have emphasized the importance of the national interest in foreign-intelligence gathering above and beyond garden-variety law enforcement, as well as the need for flexibility in the timely collection of intelligence, given the particular nature and objectives of foreign-intelligence collection. *See Duka*, 671 F.3d at 341; *In re Directives*, 551 F.3d at 1010-11; *Truong*, 629 F.2d at 912-14 (4th Cir. 1980); *[Redacted Caption]*, 2011 WL 10945618, at *24 (F.I.S.C. Oct. 3, 2011); *Mohamud*, 2014 WL 2866749, at *16-18. Indeed, both the FISC and a district court of this Circuit have so held in cases, like this one, involving intelligence collection under Section 702. *See Mohamud*, 2014 WL 2866749, at *1, 14-18; *[Redacted Caption]*, 2011 WL 10945618, at *24.

This Court should reach the same result, for the same reasons. A "significant purpose" of acquisitions under Section 702 must be, according to the statute's terms, "to obtain foreign intelligence information," 50 U.S.C. § 1881a(g)(2)(A)(v), such as information acquired to protect the Nation against foreign attacks, international terrorism, international proliferation of weapons

[9] Plaintiffs' reliance (Pls.' Mot. at 13, 15-17, 23, 25) on *Keith* and *Berger v. New York*, 388 U.S. 41 (1967), is thus misplaced because the former involves the Fourth Amendment standard for electronic surveillance in a domestic-security case, *Keith*, 407 U.S. at 324, and the latter involves the standard for an ordinary criminal case, *Berger*, 388 U.S. at 43 & n.1, 62-64.

of mass destruction, and clandestine intelligence activities of foreign intelligence services. *See id.* § 1801(e); *see also In re Directives*, 551 F.3d at 1011 (PAA, the predecessor to the FAA, had the "stated purpose" of "garnering foreign intelligence" and "[t]here [was] no indication that the collections of information [were] primarily related to ordinary criminal-law enforcement purposes"). *Cf. In re Sealed Case*, 310 F.3d at 745-46 ("programmatic purpose" of obtaining foreign intelligence was "a special need"); *Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006) (interest in preventing terrorist attacks goes "well beyond" law enforcement). Plaintiffs make no serious argument that Upstream collection is undertaken for routine law enforcement or any purpose other than furthering "legitimate national security concerns." Pls.' Mot. at 25.[10]

Upstream collection also meets the impracticability requirement of the special-needs doctrine. Congress, in fact, authorized the surveillance activities challenged here by enacting the FAA in 2008 "with a bipartisan majority" and "broad support from the intelligence community." H.R. Rep. No. 112-645(I), 112th Cong., 2d Sess., at 2 (Aug. 2, 2012), in part because the burdens imposed on the Government's limited intelligence resources and the delays occasioned by the requirement under then-current law to prepare individualized, probable-cause FISA applications for intelligence collection targeting non-U.S. persons outside the United States were undermining the Government's ability to collect such information. *See* 154 Cong. Rec. S6097, S6122 (daily ed., June 25, 2008) (statement of Senator Chambliss) ("[T]he [FAA] will fill the gaps identified by our intelligence officials and provide them with the tools and flexibility they need to collect intelligence from targets overseas."); May 1, 2007 FISA Mod. Hrg., *supra*, at 18 (testimony of DNI explaining "massive amounts of analytic resources [required] to craft FISA applications" for warrants authorizing collection of the communications of non-U.S. persons

[10] Plaintiffs do quarrel, however, that collection under Section 702 does not meet the requirements of the special-needs exception because first, the category of foreign intelligence includes "information that relates to national defense" and "foreign affairs," and second, because obtaining foreign intelligence need only be a "significant purpose" of an acquisition rather than its primary purpose. Pls.' Mot. at 25 n.24, citing 50 U.S.C. §§ 1801, 1881a(g)(2)(A)(v). But national defense and foreign affairs are Government interests just as unrelated to routine law enforcement as counter-terrorism. And, so long as the Section 702 program serves the Government's need to obtain foreign intelligence, it does not render the warrant requirement any less impracticable, or render the special-needs exception inapplicable, just because the program also promotes other legitimate governmental interests. *See, e.g.*, *Duka*, 671 F.3d at 341-45; *In re Directives*, 551 F.3d at 1011; *Mohamud*, 2014 WL 2866749, at *18.

located abroad); *see also* H.R. Rep. No. 112-645(II), 112th Cong., 2d Sess., at 2 (Aug. 2, 2012) (technological changes had made FISA "impractical" and "ineffective" in "combatting the quickly evolving threats facing our nation," whereas the FAA provided "the speed and agility necessary to meaningfully collect foreign intelligence").[11]

The courts have also long recognized that "attempts to counter foreign threats to the national security require the utmost stealth, speed, and secrecy," *Truong*, 629 F.2d at 913, and that conditioning acquisitions of foreign-intelligence information targeted at non-U.S. persons located overseas on obtaining a warrant "would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats," *id.*, "hinder the government's ability to collect time-sensitive" foreign intelligence, and thus "impede the vital national security interests that are at stake." *In re Directives*, 551 F.3d at 1011; *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 273 (S.D.N.Y. 2000) ("imposition of a warrant requirement [would] be a disproportionate and perhaps even disabling burden" on Government's ability to obtain foreign intelligence information). Courts considering the issue have found, in particular, that "application of the warrant requirement would [also] be impracticable" for acquisitions under Section 702. *Mohamud*, 2014 WL 2866749, at *18; *see also [Redacted Caption]*, 2011 WL 10945618, at *24.

Accordingly, the alleged seizure and search about which Plaintiffs complain fall under the Fourth Amendment's "special needs" exception to the warrant requirement.

2. The challenged "Stage 1" copying and "Stage 3" scanning of Plaintiffs' unretained communications are reasonable because the interests of national security far outweigh the minimal intrusion on Plaintiffs' Fourth Amendment interests.

Even where a warrant and probable cause are not required, searches and seizures remain subject to the Fourth Amendment's "traditional standards of reasonableness." *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013). In assessing the reasonableness of the putative "seizure" and "search" at Stages 1 and 3, the Court must consider the "totality of the circumstances," *Samson*

[11] The Senate Select Committee on Intelligence similarly concluded in 2012 that, without Section 702 (and the other authorities granted by the FAA) the Intelligence Community's "ability . . . to respond quickly to new threats and intelligence opportunities" would be "impede[d]." S. Rep. No. 112-174, 112th Cong., 2d Sess., at 2 (June 7, 2012).

v. California, 547 U.S. 843, 848 (2006), weighing "the promotion of legitimate governmental interests against the degree to which [the seizures and searches] intrude[] upon" Plaintiffs' protected Fourth Amendment interests. *King*, 133 S. Ct. at 1970. Applying this test, the FISA Court of Review found foreign-intelligence collection under the PAA reasonable, *In re Directives*, 551 F.3d 1012-15, and the *Mohamud* court recently found reasonable (and thus constitutional) the acquisition of foreign intelligence under Section 702, *see Mohamud*, 2014 WL 2866749, at *19-27. This Court, likewise, should conclude that the claimed seizure and search at issue here are reasonable; indeed, they infringe upon Fourth Amendment interests to a far lesser degree than the intelligence-gathering activities upheld in *In re Directives* and *Mohamud*.

The Government's national-security interest in conducting acquisitions pursuant to Section 702 "is of the highest order of magnitude." *In re Directives*, 551 F.3d at 1012; [Redacted caption], 2011 WL 10945618, at *25 (same). "[N]o governmental interest is more compelling than the security of the Nation," *Haig v. Agee*, 453 U.S. 280, 307 (1981), and combatting international terrorism, one of the principal goals of the FAA of 2008, *see* H.R. Rep. No. 112-645(I), 112th Cong., 2d Sess., at 4 (Aug. 2, 2012), "is an urgent objective of the highest order." *Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010).

To be weighed against the promotion of the compelling Government interest in protecting national security is the minimal intrusion on Plaintiffs' Fourth Amendment interest by Upstream collection as Plaintiffs allege it operates. As explained *supra*, §§ IV.A and B, the temporary creation of a copy of Plaintiffs' communications and the equally fleeting electronic scanning of communications not retained by the Government, and about which Government personnel obtain no information, produce a minimal intrusion, if any, on Plaintiffs' possessory and privacy interests, not the "massive[] intru[sion]" Plaintiffs claim. Pls.' Mot. at 24.

Any intrusion on Plaintiffs' Fourth Amendment interests is diminished further because "[s]urveillance under [Section 702] is subject to statutory conditions, judicial authorization, congressional supervision, and compliance with the Fourth Amendment," *Amnesty Int'l USA*, 133 S. Ct. at 1144, and this "matrix of [statutory] safeguards," *In re Directives*, 551 F.3d at 1013, contributes further to the program's reasonableness. *See Mohamud*, 2014 WL 2866749, at *27;

cf. King, 133 S. Ct. at 1979-80 (statutory protections guarding against further invasion of privacy contribute to reasonableness). The statute requires the DNI and the Attorney General to certify, and the FISC to approve, that a significant purpose of an acquisition is to obtain foreign intelligence information, *id.* § 1881a (g)(2)(A)(v), (i). Section 702 also requires the DNI and the Attorney General annually to certify—and the FISC to so find—that acquisitions will comply with the Fourth Amendment and the statutorily required targeting procedures are reasonably designed to target only non-U.S. persons reasonably believed to be located outside the United States, that is, those who do not have Fourth Amendment rights, *United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990). *See* 50 U.S.C. § 1881a(a), (b), (d)(2), (g), (i).[12] Along with the Executive's reports to the FISC and to Congress about "compliance with the targeting . . . procedures," *id.* § 1881a(l)(1), these requirements contribute to the reasonableness of the collection under Section 702. *See Mohamud*, 2014 WL 2866749, at *27.[13]

The Fourth Amendment requires only that the acquisitions of intelligence made possible by the alleged seizures and searches at issue here be a "reasonably effective means" of advancing the Government's goals of protecting the Nation's security. *Board of Educ. of Independent Sch. Dist. No. 92 of Pottawatomie County v. Earls*, 536 U.S. 822, 837-38 (2002). There should be no dispute here that this standard has been met and exceeded because the collection authorized by Section 702, the "primary surveillance authority granted by" the FAA, S. Rep. No. 112-229, 112th Cong., 2d Sess., at 4 (Sept. 20, 2012), has been critical to the Government's efforts to

[12] Plaintiffs are wrong to complain that the "Executive alone makes all [the] decisions" about targeting "without judicial oversight," Pls.' Mot. at 23, because the statute imposes significant limitations on permissible targeting and the purposes for which information may be collected, 50 U.S.C. § 1881a(b), (g)(2)(A)(v), and compliance with those limitations is reviewed by the FISC. *See id.* § 1881a(i); PCLOB Report at 26-28 (describing FISC's role as "extensive" in some respects). They are also wrong in dismissing the FISC's role in the process as that of "an administrative agency" instead of an Article III court. Pls.' Mot. at 21-22. The FISC determines whether the Executive is complying with the statutory requirements and the Fourth Amendment, *see* 50 U.S.C. § 1881a(i), and issues orders either approving of certifications (so directives may be issued to electronic communication service providers who must comply or challenge them, *see id.* § 1881a(h)), or disapproving the certifications so the Government is barred from conducting collections under the certifications if it does not remedy the deficiency. *Id.* § 1881a(i)(2). *See Mohamud*, 2014 WL 2866749, at *10-11.

[13] *Cf. Amnesty Int'l, USA*, 133 S. Ct. at 1150 (noting importance of requirement that the FISC "assess whether the Government's targeting and minimization procedures comport with the Fourth Amendment"); *In re Directives*, 551 F.3d at 1015 (minimization procedures reduce impact of any potential privacy intrusions).

combat international terrorism and other threats to the United States and its interests abroad. *See* S. Rep. No. 112-174, 112th Cong., 2d Sess., at 2 (June 7, 2012) (describing collections under the FAA as "critical"); H.R. Rep. No. 112-645(I), 112th Cong., 2d Sess., at 2 (Aug. 2, 2012) (FAA authorities "critical" and "allow[] intelligence professionals to more quickly and effectively monitor terrorist communications"); H.R. Rep. No. 112-645(II), 112th Cong., 2d Sess., at 3 (Aug. 2, 2012) (emphasizing "critical import[ance]" of the FAA).

In recommending re-authorization of the FAA in 2012, for example, the House Committee on Intelligence, which "held two hearings and multiple classified briefings" on the efficacy of surveillance under the FAA, found that the:

> importance of the collection of foreign intelligence under the [FAA] . . . cannot be underscored enough. In short, intelligence collected under the FAA is critically important to maintaining our national security. The information collected under this authority is often unique, unavailable from any other source, and regularly provides critically important insights and operationally actionable intelligence on terrorists and foreign intelligence targets around the world.

H.R. Rep. No. 112-645(II), 112th Cong., 2d Sess., at 3, 5 (Aug. 2, 2012); *see also* PCLOB Report at 124 (finding that Upstream collection "has unique value"). Similarly, the Senate Select Committee on Intelligence found—based on "numerous hearings" and years of briefings by Executive Branch officials—that "the authorities provided under the [FAA] have greatly increased the government's ability to collect information and act quickly against important foreign intelligence targets." S. Rep. No. 112-174, 112th Cong., 2d Sess., at 2 (June 7, 2012).[14]

The Executive Branch's assessment of the value and importance of intelligence-gathering activities authorized under the FAA is "entitled to deference." *Humanitarian Law Project*, 561 U.S. at 32-34. On a daily basis the Executive Branch confronts an array of constantly evolving threats to national security, and is charged with making difficult judgments about how best to counter those threats. *See id.; Truong*, 629 F.2d at 914 (Executive has "superior expertise" in

[14] Indeed, even those members of the House Judiciary Committee who "strongly oppose[d]" reauthorization, H.R. Rep. No. 112-645(I), 112th Cong., 2d Sess., at 13 (Aug. 2, 2012) (dissenting views), recognized "[w]ithout question" that the FAA provided the intelligence community with an "important tool" to "collect significant and valuable foreign intelligence." *Id.* at 17 (dissenting views). The same was true of the minority views expressed in the report by the House Permanent Select Committee on Intelligence. *See* H.R. Rep. No. 112-645(II), 112th Cong., 2d Sess., at 10 (Aug. 2, 2012) (minority views).

foreign intelligence and is "constitutionally designated as the pre-eminent authority in foreign affairs"). Congress's judgment regarding the value and importance of intelligence acquisitions authorized under the FAA, as reflected in its 2012 reauthorization of these authorities—including Section 702—*see* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631, is also entitled to the courts' respect. *Humanitarian Law Project*, 561 U.S. at 33-35; *see also Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) ("A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.").[15]

Each court to consider the question has concluded that the Government's compelling interest in protecting national security justifies the arguably greater intrusion of electronic surveillance under Section 702, and its predecessor, the PAA, on the privacy of those individuals whose electronic communications are, in fact, retained by the Government and are subject to further review and scrutiny by Government officials. *See In re Directives*, 551 F.3d at 1012-16 (finding that the PAA, which authorized surveillance of U.S. persons abroad (and was thus broader than the FAA), "constitute[d] a sufficiently reasonable exercise of governmental power to satisfy the Fourth Amendment"); *Mohamud*, 2014 WL 2866749, at *24-27 (Section 702 acquisition and "subsequent querying" of that surveillance collection is reasonable under the Fourth Amendment). All the more so, the promotion of the Government's national-security interests through Upstream collection justifies the minimal intrusions on Plaintiffs' Fourth Amendment interests in communications that are not among those the Government retains.[16]

---

[15] The conclusions reached by Congress about the value of Section 702 and other FAA intelligence-gathering authorities are echoed in other public reports. *See* PCLOB Report at 2, 104, 107, 110 (July 2, 2014) (Section 702 "valuable and effective"; "provides a degree of flexibility not offered by comparable surveillance authorities"; "help[s] the United States learn more about the membership, leadership structure, priorities, tactics, and plans of international terrorist organizations," leading "to the discovery" and "disruption" of "previously unknown terrorist plots"; and has been "highly valuable" in serving "other foreign intelligence and foreign policy goals"); The President's Review Group on Intelligence and Communications Technologies, *Liberty & Security in a Changing World*, 145 (Dec. 12, 2013) (Exh. D, hereto) ("[S]ection 702 has clearly served an important function in helping the United States to uncover and prevent terrorist attacks both in the United States and around the world.").

[16] Courts have reached similar conclusions in other national-security contexts, all involving arguably greater intrusions on Fourth Amendment interests than Plaintiffs have shown. *See also In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 172-77 (2d Cir. 2008) (warrantless and broad electronic surveillance of U.S. citizen abroad constitutional

At bottom, even if Plaintiffs had presented competent evidence to support the conclusion that Fourth Amendment seizures and searches occur when Plaintiffs' online communications are fleetingly copied while transiting the Internet backbone, and then the copies electronically scanned and destroyed in real time—all without the Government retaining or learning anything about the communications involved—those searches and seizures fall within the foreign-intelligence exception to the warrant requirement, and are reasonable under the totality of the circumstances. Thus no violation of the Fourth Amendment takes place.

D. Even if Plaintiffs Had Presented Evidence of a Seizure or Search, Not Justified Under the Special Needs Doctrine, Their Fourth Amendment Claim Still Could Not Be Litigated Without National-Security Information Protected by the State Secrets Privilege.

Even if the Court were to conclude that Plaintiffs have presented sufficient admissible evidence of facts, which, if true, would demonstrate that Upstream collection involves a Fourth Amendment seizure or search of Plaintiffs' communications, and that the minimal intrusion upon Plaintiffs' possessory and privacy interests is not far outweighed by Upstream collection's promotion of the Government's compelling interest in national security, then the Government, in the alternative, would still be entitled to summary judgment on Plaintiffs' Fourth Amendment claims. That is so, because adjudication of those claims and the Government's defenses thereto would require disclosure of national-security information subject to the DNI's assertion of the state secrets privilege.

Previously in this litigation the DNI asserted the state secrets privilege over "[a]ny information concerning NSA intelligence activities, sources, or methods that may relate to or be necessary to adjudicate plaintiffs' allegations," Public Decl. of James R. Clapper, DNI (Sept. 11, 2012) (ECF No. 104) ¶ 10.C; *see* Public Decl. of Frances J. Fleisch, NSA (Sept. 11, 2012) (ECF No. 105) ¶ 14.B, and renewed that assertion of privilege over "information concerning the scope

because the government's need to "intrude was even greater" than the intrusion); *Cassidy*, 471 F.3d at 70 (searches of carry-on luggage and vehicles before boarding ferries); *MacWade v. Kelly*, 460 F.3d 260, 269-75 (2d Cir. 2006) (random search of subway passengers' baggage). Indeed, given the national-security interests at stake, and the minute extent of any infringement on Fourth Amendment interests at alleged Stages 1 and 3, the balance tips even further in the Government's favor than in previous "special needs" cases where the Supreme Court has readily upheld, for example, DNA testing, for identification purposes, of persons taken into custody, *King*, 133 S. Ct. at 1979-80, and suspicionless urinalysis testing of high-school athletes to combat drug abuse. *Earls*, 536 U.S. at 832-34.

and operational details of NSA intelligence activities that may [be] relat[ed] to or be necessary to adjudicate plaintiffs' allegations," including "operational details related to the collection of communications under FISA section 702." Public Decl. of James R. Clapper, DNI (Dec. 20, 2013) (ECF No. 168) ¶¶ 19.C.1.b, 35 ("Dec. 20, 2013 Clapper Decl."); *see* Public Decl. of Frances J. Fleisch, NSA (Dec. 20, 2013) (ECF No. 169) ¶¶ 35.B.1.b, 38, 39. This Court, in *Jewel*, 965 F. Supp. 2d at 1103, held that "the evidence submitted thus far that the [G]overnment seeks to protect from disclosure contain[s] valid state secrets 'which, in the interest of national security, should not be divulged'" (quoting *United States v. Reynolds*, 345 U.S. 1, 10 (1953)).

As explained in the classified supplement submitted *in camera, ex parte*, herewith, the NSA possesses information "concerning operational details related to the collection of communications under FISA section 702," Dec. 20, 2013 Clapper Decl. ¶ 19.C.1.b, that are necessary to a determination of Plaintiffs' seizure and search claims, and the Government's defense thereto. Those facts are set forth in the Classified Decl. of Miriam P., NSA (Sept. 29, 2014), also submitted *in camera, ex parte*, herewith; and as confirmed by the DNI, they fall within the scope of his assertion of the state secrets privilege, already made in this case, over the operational details of the Section 702 program. Decl. of James R. Clapper, DNI (Sept. 29, 2014) (Exh. E, hereto) ¶ 2.

When, as here, a court has sustained a claim of state secrets privilege, the evidence subject to the privilege is "completely removed from the case," *Kasza*, 133 F.3d at 1166, and the court must then resolve "how the matter should proceed in light of the successful privilege claim." *Al-Haramain Islamic Found. v. Bush*, 507 F.3d 1190, 1202 (9th Cir. 2007) (citation and internal quotation marks omitted): *Jewel*, 965 F. Supp. 2d at 1101. In many situations the exclusion of the privileged evidence will have "'no consequences save those resulting from the loss of the evidence,'" and "'the case will proceed accordingly,'" *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1082-83 (9th Cir. 2010) (*en banc*) (quoting *Al-Haramain*, 507 F.3d at 1204). In some circumstances, however, "application of the privilege may require dismissal of the action," if, for example, "'the privilege deprives the plaintiff of information needed to set forth a prima facie case, or the defendant of information that would otherwise give

the defendant a valid defense to the claim . . . .'" *Id.* at 1083 (quoting *Kasza*, 133 F.3d at 1166); *Jewel*, 965 F. Supp. 2d at 1100.

Here, as explained in the classified *in camera, ex parte* supplement submitted herewith, if the Court were to determine that Plaintiffs have presented competent evidence from which it could be found that either a seizure or search of Plaintiffs' communications occurs in the Upstream collection process, and that the minimal intrusion on Plaintiffs' Fourth Amendment interests is not outweighed by the contribution of Upstream collection to national security, then the operational details presented in the Classified Miriam P. Declaration would be necessary to a full and fair adjudication of Plaintiffs' Fourth Amendment claim, including the Government's ability to raise and support defenses in addition to those presented herein. That information, however, is excluded from the case due to the DNI's valid assertion of the state secrets privilege. *Kasza*, 133 F.3d at 1166. Accordingly, even barring all other grounds discussed herein on which Plaintiffs' motion should be denied, the state secrets doctrine would require that Plaintiffs' claims be dismissed and judgment awarded instead to the Government. *Jeppesen*, 614 F.3d at 1083; *Kasza*, 133 F.3d at 1166; *Jewel*, 965 F. Supp. 2d at 1100; *see Tenenbaum v. Simonini*, 372 F.3d 776, 777 (6th Cir. 2004).[17]

CONCLUSION

For the foregoing reasons, Plaintiffs' motion for partial summary judgment on their Fourth Amendment claim should be denied, and judgment awarded instead to the Government on Plaintiffs' Fourth Amendment claim as a matter of law.

[17] The Court's prior conclusion that the privilege is displaced by 50 U.S.C. § 1806(f), *Jewel*, 965 F. Supp. 2d at 1105-06, with which the Government respectfully continues to disagree, does not alter this conclusion. As the Government explained in response to the Court's four threshold questions, Plaintiffs must first establish that they are "aggrieved persons" under § 1806(f) before its procedures can be used to determine the legality of electronic surveillance, and notwithstanding recent Government disclosures, a § 1806(f) proceeding and an ensuing court decision risk disclosure of still-classified information that could cause exceptionally grave damage to national security. *See* Gov. Defs.' Reply on Threshold Legal Issues at 4-14 (ECF No. 185). Moreover, Plaintiffs have expressly declined the use of § 1806(f) proceedings at this time, choosing instead to file a motion "based entirely on public evidence" and "defer section 1806(f) proceedings." Plaintiffs' Responses to the Court's Four Questions at 7 (ECF No. 177). Lastly, the Court held that § 1806(f) displaces the state secrets privilege "with regard to matters within FISA's purview," *Jewel*, 960 F. Supp. 2d at 1106, but there are no FISA claims against the Government left in this case. *See* Joint Case Management Statement at 6-7 (ECF No. 159).

Dated: September 29, 2014

Respectfully Submitted,

JOYCE R. BRANDA
Acting Assistant Attorney General

JOSEPH H. HUNT
Director, Federal Programs Branch

ANTHONY J. COPPOLINO
Deputy Branch Director

/s/ James J. Gilligan
JAMES J. GILLIGAN
Special Litigation Counsel
MARCIA BERMAN
Senior Trial Counsel
RODNEY PATTON
JULIA BERMAN
Trial Attorneys

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, N.W., Room 6102
Washington, D.C. 20001

Phone: (202) 514-3358
Fax: (202) 616-8470
E-mail: james.gilligan@usdoj.gov

Attorneys for the Government Defendants